A THEORY OF CROSSED CHARACTERS

BY

REINHOLD BAER

The characters of the finite group[1] G in the cyclic group E of order[2] m are just the multiplicative, single-valued G to E functions. To define crossed characters we have to consider apart from G and E a homomorphism C of G into the group of automorphisms of E; and we denote the map of the element g in G under C also by g. A single-valued G to E function $f(g)$ is termed a C-character (or a crossed character) of G, if it is a solution of the following functional equation [3]: $f(uv)=f(u)^v f(v)$ for u and v in G. The C-characters, like the ordinary characters of G, form a finite abelian group, the C-character group[4] of G; and as in the classical theory of characters one aims at establishing a duality between G and its C-character group. But here the similarity ends. For in the classical theory the following three properties are equivalent: (a) 1 is the only element in G which is mapped upon 1 by every character of G; (b) it is possible to establish a duality between G and its character group; (c) G and its character group are isomorphic. But if one substitutes in these properties C-characters for the ordinary characters, no such equivalence holds. Though still (c) implies (b) and (b) implies (a), only a few of the groups satisfying (a) meet the requirement (b); and only rarely a group satisfying (b) may be shown to satisfy (c).

Presented to the Society April 24, 1943; received by the editors December 21, 1942.

(1) Only *finite* groups will be considered in this investigation; for this reason we shall use the term "group" always in the sense of "finite group."

(2) It will be apparent immediately why it is not advisable to consider some "absolute" value group like the group of all the roots of unity.

(3) Apparently the first to investigate this functional equation was I. Schur. Recently functions meeting this requirement have been termed crossed characters, though it might have been more in conformity with accepted usage to term them "crossed homomorphisms" and to reserve the term "crossed character" for the crossed homomorphisms with values in a cyclic group. For investigations of this functional equation; see I. Schur, *Über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. vol. 127 (1904) pp. 20–50; I. Schur, *Bemerkungen zu der vorstehenden Arbeit des Herrn Speiser*, Math. Zeit. vol. 5 (1919) pp. 7–10; A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeit. vol. 5 (1919) pp. 1–6; R. Baer, *Automorphismen von Erweiterungsgruppen*, Actualités Scientifiques et Industrielles no. 205, 1935; S. MacLane and O. F. G. Schilling, *Normal algebraic number fields*, Trans. Amer. Math. Soc. vol. 50 (1941) pp. 295–384; A. H. Clifford and S. MacLane, *Factor sets of a group in its abstract unit group*, Trans. Amer. Math. Soc. vol. 50 (1941) pp. 385–406; S. MacLane and O. F. G. Schilling, *A general Kummer theory for function fields*, Duke Math. J. vol. 9 (1942) pp. 125–167.

(4) The C-character group of the Galois group of an algebraic extension is of importance in the theory of radical extensions as will be shown elsewhere.

In Chapter III of this investigation we characterize those groups G and homomorphisms C which meet the requirement (a); and those satisfying conditions (b) or (c) are determined in Chapter V. In Chapter II the order of the C-character group is evaluated and conditions for equality of the orders of G and of its C-character group are derived; this latter property is later seen to be intermediate between (b) and (c). Chapter IV is devoted to a characterization of the groups G and homomorphisms C satisfying the following postulate: the C-character group of G is the only group T of C-characters of G such that 1 is mapped upon 1 by every C-character in T. This property stands between (a) and (b) and is important by its applications to the theory of radical extensions of fields(5).

Chapter I. Preliminaries

I. 1. **The classical theory of characters.** In this section we give a resumé of the classical theory of characters of finite abelian groups in the form best suited to our purposes; and we indicate how to derive these statements from the theorems customarily found in the various texts(6).

If G is a finite (not necessarily abelian) group, and if E is a cyclic group of order m, then a *character of G in E* is a single-valued G to E function $f(g)$ satisfying the functional equation $f(g)f(h)=f(gh)$ for g and h in G; in short, a character of G in E is a homomorphism of the group G into the cyclic group E. If f' and f'' are characters of G in E, then $f'(g)f''(g)$ is a character of G in E which is called the product $f'f''$ of these characters. It is readily seen that the system of all the characters of G in E is a finite abelian group, the character group of G in E.

Basic for many constructions of characters is the following *extension principle.*

Lemma I.1.1. (a) *If S is a normal subgroup of the group G, and if f is a character of the quotient group G/S in E, then there exists one and only one character of G in E which maps S upon* 1 *and which induces f in G/S.*

(b) *If G is an abelian group the orders of whose elements are divisors of m, if f is a character of the subgroup S of G in E, then there exists a character of G in E which induces f in S.*

We denote by G' *the commutator subgroup of* G and by G^m the subgroup of G which is generated by all the mth *powers of elements in* G.

Theorem I.1.2. *$G'G^m$ is the subgroup of all the elements in G which are mapped upon* 1 *by every character of G in E.*

To prove this theorem one notes first that the characters of G in E are

(5) This application of the present theory will be treated elsewhere.

(6) For example, E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig, 1923, in particular §10.

homomorphisms of the group G into a cyclic group of order m, and that homomorphisms of this kind map both G' and G^m upon 1; and one deduces from Lemma I.1.1 that there exists to every element not in $G'G^m$ a character of G in E which does not map it upon 1.

THEOREM I.1.3. *If G is a finite group and E a cyclic group of order m, then each of the following properties implies the others:*

(1) *1 is the only element in G which is mapped upon 1 by every character of G in E.*

(2) *G is an abelian group the orders of whose elements are divisors of m.*

(3) *G and its character group in E are isomorphic groups.*

The equivalence of (1) and (2) is essentially a restatement of Theorem I.1.2. Property (2) is a consequence of (3), since the character group of G in E is abelian, and since the mth power of every character of G in E is 1. That (2) implies (3) is a classical theorem([7]).

If S is a subgroup of G, then we denote by $K(S)$ the group of all the characters f of G in E which map S upon 1, that is, $K(S) = \{f(S) = 1\}$; and if T is a group of characters, then we denote by $G(T)$ the set of all the elements g in G which are mapped upon 1 by every character in T, that is, $G(T) = \{T(g) = 1\}$.

THEOREM I.1.4([8]). *If G is a finite abelian group the orders of whose elements are divisors of m, if E is a cyclic group of order m, then*

(a) *$G(K(S)) = S$ for every subgroup S of G;*

(b) *$K(G(T)) = T$ for every group T of characters of G in E;*

(c) *mapping the subgroup S of G upon $K(S)$ constitutes a duality([9]) of G upon the character group of G in E.*

REMARK. If T is a group of characters such that $G(T) = 1$, then every character of G is contained in T.

I. 2. **Fundamental concepts.** We are concerned with a cyclic group E of order m and a homomorphism C of the finite group G into the group of automorphisms of E. We shall use the same symbol g for the element g in the group G and the automorphism which corresponds to g under C, or as we shall say, the automorphism of E induced by the element g in G. Every automorphism of E consists in raising every element in E to a fixed power which is prime to m and which is uniquely determined modulo m; this integer (modulo m) which corresponds to the automorphism induced by the element g in G also shall be denoted by g.

The elements in G which are mapped upon the identity automorphism of

([7]) See, for example, Hecke, op. cit. p. 36.

([8]) See, for example, Hecke, op. cit. pp. 36–38.

([9]) A *duality* is a monotone decreasing, 1:1 correspondence between the elements in two partially ordered sets.

E by C form a normal subgroup G_C of G; and G/G_C is essentially the same as a group of automorphisms of the cyclic group E. This implies in particular the commutativity of G/G_C.

It will be convenient to denote by C_0 the homomorphism of G which maps every element in G upon the identity automorphism of E; clearly C_0 is characterized by $G_{C_0}=G$.

The cyclic group E of order $m=\prod_p p^{m(p)}$ is the direct product of (uniquely determined) cyclic groups $E(p)$ of prime power order $p^{m(p)}$. Every automorphism of E induces an automorphism in every $E(p)$. If p is some prime, then we denote by Cp the homomorphism of G which maps the element g in G upon the automorphism of $E(p)$ which the automorphism g of E induces in $E(p)$. It is readily seen that G_C *is the cross-cut of all the* G_{Cp}.

A C-character of G *(in* E*) is a single-valued* G *to* E *function* $f(g)$ *which satisfies the functional equation* $f(gh)=f(g)^h f(h)$ *for* g *and* h *in* G. Clearly the C_0-characters of G are just the ordinary characters of G in E which we discussed in I.1.

If f' and f'' are C-characters of G, then $f'(g)f''(g)$ may be verified to be a C-character too; and this C-character of G is termed the product $f'f''$. The set of all C-characters of G thus forms a finite abelian group, *the C-character group* $L=L(G, C)$ *of* G; and the orders of the C-characters of G are divisors of the order m of E.

The order of a C-character f of G is a power of the prime number p if, and only if, f is at the same time a Cp-character of G, since f is of order a power of p if, and only if, f maps G upon a subgroup of $E(p)$.

If v is any element in E, then $f(g)=v^{1-g}$ for g in G is a C-character of G, since $v^{1-gh}=v^{1-h}v^{h-gh}=(v^{1-g})^h v^{1-h}$. Such C-characters of G have been termed *unit or principal characters*; and the group of all these characters may be called the *principal genus*. It is a cyclic group which is generated by the unit character e^{1-g} for e a generator of the cyclic group E.

LEMMA I.2.1. *If* f *is a* C*-character of* G*, and if* $G(f)$ *is the set of all the elements* g *in* G *which satisfy* $f(g)=1$*, then* (a) $G(f)$ *is a subgroup of* G*, and* (b) $f(g)=f(h)$ *if, and only if,* gh^{-1} *is in* $G(f)$.

REMARK. It is easy to construct examples of C-characters f such that $G(f)$ is not a normal subgroup of G.

Proof. If g and h are both in $G(f)$, then $f(gh)=f(g)^h f(h)=1$ so that gh also belongs to $G(f)$, proving (a). From $1=f(1)=f(hh^{-1})=f(h)^{h^{-1}}f(h^{-1})$ one infers that $f(gh^{-1})=f(g)^{h^{-1}}f(h^{-1})=(f(g)f(h)^{-1})^{h^{-1}}$ and this makes contention (b) evident.

LEMMA I.2.2. *If the automorphism* a *of the group* G *has the property that* g *and* g^a *are mapped by* C *upon the same automorphism of* E*, then the function* $f^a(x)=f(x^a)$ *is a* C*-character of* G *whenever* $f(x)$ *is a* C*-character of* G*; and in this*

fashion the automorphism a of G induces an automorphism a of the C-character group of G.

REMARK. The inner automorphisms of G meet the requirement imposed upon the automorphism a in the lemma, since the group of automorphisms of the cyclic group E is abelian.

Proof. If f is a C-character of G, and if g and g^a induce the same automorphism of E, then $f^a(gh)=f(g^ah^a)=f(g^a)^{h^a}f(h^a)=f^a(g)^hf^a(h)$, as was to be shown.

If p is a prime number, then we denote by $H(p)=H(G, p)$ *the set of all the elements g in G which are mapped upon* 1 *by all the Cp-characters of G.* It is a fairly immediate consequence of Lemma I.2.2. that $H(p)$ is a normal subgroup of G, since with $f(x)$ every $f(g^{-1}xg)=f'(x)$ for g in G is a Cp-character of G.

The cross-cut H of all the $H(p)$ is just the set of all the elements g in G which are mapped upon 1 by every C-character of G, since every C-character of G is a product of Cp-characters of G, as the Cp-characters of G are exactly the C-characters of order a power of p.

The cross-cut $\overline{H}(p)$ of all the $H(q)$ for $q\neq p$ will prove important occasionally; this normal subgroup of G is readily seen to consist of all those elements g in G which are mapped upon elements in $E(p)$ by every C-character of G.

The determination of the subgroups $H(p)$ will be one of our most important problems (see III.2 below); in this direction we now prove the following statement.

LEMMA I.2.3. $H(p)\leqq G_{Cp}$ *for every prime number p.*

Proof. If the element g in G does not belong to G_{Cp}, then it induces in $E(p)$ an automorphism which does not leave every element invariant. Thus there exists in $E(p)$ an element v such that $v\neq v^g$. The C-character $f(x)=v^{1-x}$ is a Cp-character and satisfies $f(g)\neq 1$ so that g does not belong to $H(p)$.

COROLLARY I.2.4. $H\leqq G_C$.

This is an immediate consequence of Lemma I.2.3, since G_C is the cross-cut of the G_{Cp}, and since H is the cross-cut of the $H(p)$.

I. 3. **C-complete groups and the extension of C-characters.** The group G is termed *C-complete*, if 1 is the only element in G which is mapped upon 1 by every C-character of G, that is, if the subgroup H, introduced in I.2, is equal to 1.

THEOREM I.3.1. *The group G is C-complete if, and only if, the following three conditions are satisfied by G and C:*

(i) *G_C is abelian;*
(ii) *the orders of the elements in G_C are divisors of the order m of E;*
(iii) *every (C_0-)character of G_C in E is induced by a C-character of G.*

Proof. Every C-character of G induces in G_C an ordinary, that is, a C_0-character in E. If G is C-complete, then 1 is the only element in G_C mapped upon 1 by every C_0-character of G_C which is induced by C-characters of G. The necessity of conditions (i), (ii) is now a consequence of Theorem I.1.3 and the necessity of condition (iii) may be deduced from Theorem I.1.4.

Assume conversely that conditions (i) to (iii) are satisfied by G and C. It is a consequence of Corollary I.2.4 that only elements in G_C are mapped upon 1 by every C-character of G. If $g \neq 1$ is an element in G_C, then we infer from conditions (i), (ii) and Theorem I.1.4 the existence of a C_0-character d of G_C in E such that $d(g) \neq 1$; and there exists by (iii) a C-character f of G, inducing d in G_C, so that in particular $f(g) \neq 1$. Hence G is C-complete.

COROLLARY I.3.2. *If G is C-complete, then*
(iv) *$g^{-1}xg = x^g$ for x in G_C and g in G where the exponent g is the modulo m uniquely determined integer corresponding to the element g under C.*

Proof. If x and y are elements in G_C, and if g is an element in G, then g and xgy induce the same automorphism in E. Hence C-characters f of G satisfy $f(g^{-1}xgx^{-g}) = f(g^{-1})^{xgx^{-g}} f(x)^{gx^{-g}} f(g)^{x^{-g}} f(x^{-g}) = f(g^{-1})^g f(g) f(x)^g f(x^{-g}) = f(g^{-1}g) f(x)^g f(x)^{-g} = 1$, since f is a C_0-character on G_C, and since x and x^{-g} are in G_C. Thus $g^{-1}xgx^{-g}$ is mapped upon 1 by every C-character of G; and this implies $g^{-1}xgx^{-g} = 1$, since G is C-complete, as was to be shown.

REMARK. If S is a subgroup of G_C, and if the conditions (i), (ii), (iv) are satisfied by G and C, then *S is a normal subgroup of G.*

LEMMA I.3.3. *If the normal subgroup S of G is part of G_C, then the homomorphism C of G induces a homomorphism C of G/S; and every C-character of G/S is induced by one and only one C-character of G which maps S upon* 1.

The proof is obvious.

LEMMA I.3.4. *If the conditions* (i), (ii), (iv) *are satisfied by G and C, if S is a subgroup of G_C and T a subgroup of G such that $G = ST$, if the C-characters s and t of S and T respectively coincide on the cross-cut $S \cap T$ of S and T, then there exists one and only one C-character of G which induces s in S and t in T.*

Proof. Every element g in G has the form uv for u in S and v in T since S is a normal subgroup of $G = ST$. If u, u' are elements in S and v, v' elements in T such that $uv = u'v'$, then v and v' induce the same automorphism in E, $u^{-1}u' = vv'^{-1}$ is an element in $S \cap T$, and s is a C_0-character in S; and hence we find that

$$s(u)^v t(v) = s(u)^v t(vv'^{-1}v') = s(u)^v t(vv'^{-1})^{v'} t(v')$$
$$= s(u)^{v'} s(u^{-1}u')^{v'} t(v') = s(u')^{v'} t(v').$$

This shows that $f(uv) = s(u)^v t(v)$ for u in S and v in T is a single-valued G to E function.

If u, u' are in S and v, v' are in T, then

$$f(uvu'v') = f(uvu'v^{-1}vv') = f(uu'^{v^{-1}}vv') = s(uu'^{v^{-1}})^{vv'} t(vv')$$
$$= s(u)^{vv'} t(v)^{v'} s(u'^{v^{-1}})^{vv'} t(v')$$
$$= [s(u)^v t(v)]^{v'} s(u')^{v'} t(v') = f(uv)^{v'} f(u'v')$$
$$= f(uv)^{u'v'} f(u'v'),$$

proving that f is the desired C-character of G.

That f is the only C-character of G meeting our requirements is obvious; and likewise it is obvious that the condition of the equality of s and t on $S \cap T$ is indispensable.

If the conditions (i), (ii) and (iv) are satisfied by the group G and the homomorphism C, then there exists one and essentially only one smallest group M which contains G_C and which is a direct product of cyclic groups of order m. If x is an element in G, then there corresponds to x under C a modulo m uniquely determined integer x; and thus y^x is a well determined element in M, whenever x is in G and y is in M. There exists therefore one and essentially only one group V which contains G and M as subgroups, satisfies $V = MG$ and the rule $x^{-1}yx = y^x$ for x in G and y in M. This group V we shall always denote by MG; and we note that M is a normal subgroup of MG whose cross-cut with G is exactly G_C.

THEOREM I.3.5. *If the conditions* (i), (ii) *of Theorem* I.3.1 *and condition* (iv) *of Corollary* I.3.2 *are satisfied by the group G and the homomorphism C, then the following property of MG is a necessary and sufficient condition for C-completeness of G:*

(v) *There exists a subgroup R of MG such that* $MG = MR$ *and* $M \cap R = 1$.

REMARK. The elements of the subgroup R figuring in (v) form a set of representatives of the cosets of MG modulo M. Borrowing a term from the theory of extensions one may therefore restate (v) as follows: *M splits G.*

Proof. Since $M \cap G = G_C$, there exists a uniquely determined homomorphism of MG into the group of automorphisms of E which coincides with C on G and which maps every element in M upon the identity automorphism. This extension of the homomorphism C we denote by C too; and we mention that $(MG)_C = M$.

(+) *G is C-complete if, and only if, MG is C-complete.*

If MG is C-complete, then G is C-complete, since every C-character of MG

induces a C-character in its subgroup G. If conversely G is C-complete, and if f_0 is a C_0-character of M in E, then f_0 induces in G_C a C_0-character f_1; and we infer from Theorem I.3.1 (iii) the existence of a C-character f_2 of G which induces f_1 in G_C. Since f_0 and f_2 coincide on the cross-cut G_C of M and G, since $M=(MG)_C$, and since conditions (i), (ii), (iv) are satisfied by MG and C, we deduce from Lemma I.3.4 the existence of a C-character f of MG which coincides with f_2 on G and with f_0 on M. Thus conditions (i), (ii), (iii) of Theorem I.3.1 are satisfied by MG and C; and MG is C-complete, if G is C-complete.

(++) *MG is C-complete if, and only if, condition* (v) *is satisfied by MG.*

If condition (v) is satisfied by MG, then there exists a subgroup R of MG such that $MG=MR$ and $M\cap R=1$. Since conditions (i), (ii) and (iv) are satisfied by MG and C, and since $(MG)_C=M$, we deduce from Lemma I.3.4 that every C_0-character of M in E is induced by one and only one C-character of MG which maps R upon 1. Thus conditions (i), (ii), (iii) are satisfied by MG and C; and we have shown that the C-completeness of MG is a consequence of condition (v).

For the proof of the converse we need two lemmas which will prove useful in later investigations. If g is an element in G and f a C-character of G, then we put:

$$(*) \qquad F_g(f) = f(g).$$

LEMMA I.3.5.1. *F_g is, for every g in G, an ordinary character of the C-character group of G in E.*

This is an immediate consequence of the definition of product of C-characters.

LEMMA I.3.5.2. *If G is C-complete, then $g'=g''$ is a necessary and sufficient condition for $F_{g'}=F_{g''}$.*

$F_{g'}=F_{g''}$ if, and only if, $f(g')=f(g'')$ for every C-character f of G. We deduce from Lemma I.2.1 that this is the case if, and only if, $f(g'g''^{-1})=1$ for every C-character f of G; and this last fact is equivalent to $g'=g''$, since G is C-complete.

We suppose now that MG be C-complete; and we denote by K the C-character group of MG, by L the group of ordinary characters of K in E. It is a consequence of Lemma I.3.5.1 that F_x for x in MG is an element in L. If r, s are elements in M, then $F_{rs}(f)=f(rs)=f(r)^sf(s)=f(r)f(s)=F_r(f)F_s(f)$ or $F_{rs}=F_rF_s$; and we infer from Lemma I.3.5.2 that F_y is an isomorphism of M upon the subgroup F_M of L, since MG is C-complete. Since E is of order m, it follows that $L^m=1$. Since M and therefore F_M is a direct product of cyclic groups of the maximum order m in L, it follows that F_M is a direct factor of L,

proving the existence of a subgroup L' of L such that L is the direct product of F_M and L'.

We select in every coset X of MG/M a representative $r(X)$, in particular $r(M)=1$. If A and B are cosets of MG/M, then $(A, B)=(rAB)^{-1}r(A)r(B)$ is an element in M. Considering that C maps all the elements in the coset X upon the same automorphism X of E, we find for every C-character f of MG:

$$\begin{aligned} F_{r(AB)}F_{(A,B)}(f) &= f(r(AB))f((A, B)) = f(r(A, B))^{(A,B)}f((A, B)) \\ &= f(r(AB)(A, B)) = f(r(A)r(B)) = f(r(A))^{B}f(r(B)) \\ &= F^{B}_{r(A)}F_{r(B)}(f). \end{aligned}$$

Since $F_{r(X)}$ is an element in the direct product L of F_M and L', there exist elements $c(X)$ in M and $c'(X)$ in L' such that $F_{r(X)}=F_{c(X)}c'(X)$. Since (A, B) is in M, since the cross-cut of L' and F_M is 1, we deduce now that $c'(AB)=c'(A)^{B}c'(B)$ and that $F_{c(AB)}F_{(A,B)}=F^{B}_{c(A)}F_{c(B)}$. Since we have shown before that F effects an isomorphism between M and F_M, we may infer from the last identity the following equation: $c(AB)(A, B)=c(A)^{B}c(B)$ for A, B in GM/M.

Now we introduce new representatives of the cosets of MG/M by the definition: $r'(X)=r(X)c(X)^{-1}$ for X in MG/M. Then

$$\begin{aligned} r'(AB) &= r(AB)c(AB)^{-1} = r(AB)(A, B)c(A)^{-B}c(B)^{-1} \\ &= r(A)r(B)c(A)^{-B}c(B)^{-1} = r(A)c(A)^{-1}r(B)c(B)^{-1} \\ &= r'(A)r'(B); \end{aligned}$$

and this shows that the representatives $r'(X)$ of MG/M form a subgroup of MG, that is (v) is satisfied by MG. This completes the proof of (++); and our theorem is an immediate consequence of (+) and (++).

The criterion (v) for C-completeness has the disadvantage of not being an "interior" property of G, since it involves extensions of the group G. This makes this criterion hard to handle in applications and for this reason we shall attack the problem from a different angle in Chapter III, in particular Theorem III.3.3.

The last paragraph of the proof of Theorem I.3.5 as well as the criterion (v) contain a comparatively simple method for actual construction of C-complete groups. This may be indicated briefly: If G is a C-complete group, then G_C is an abelian group which we shall denote by B, and B is part of the group M which is a direct product of cyclic groups of order m. The quotient group G/G_C is a group A of automorphisms of the cyclic group E of order m and is at the same time a group of automorphisms of M, since we may identify every element x in A with an integer modulo m that is prime to m. To determine G completely as an extension of B by A, realizing the given automorphisms of B, we need only the "factor sets" (a, b) for a and b in A which had been discussed in the last paragraph of the proof of Theorem I.3.5, and criterion

(v) states—as has been pointed out during this proof—exactly that there exists a single-valued A to M function $c(x)$, satisfying:

$$(**) \qquad c(x)^{v}c(y) = c(xy)(x, y) \qquad \text{for } x \text{ and } y \text{ in } A.$$

Putting $h(x)=Bc(x)$ for x in A we obtain a single-valued A to M/B function satisfying $h(x)^{v}h(y)=h(xy)$ for x, y in A, that is a crossed homomorphism of A into M/B.

If $c'(x)$ is another solution of the functional equation (**), then the function $c''(x)=c'(x)c(x)^{-1}$ satisfies $c''(x)^{v}c''(x)=c''(xy)$, and is therefore a crossed homomorphism of A into M. Passing from the factor set (a, b) to an "associated" factor set $(a, b)'=b(y)^{-1}b(x)^{-v}b(xy)(x, y)$ for $b(z)$ in B clearly does not change the crossed homomorphisms of A into M/B at all.

That conversely every crossed homomorphism of A into M/B may be realized in the fashion just described is readily seen.

Chapter II. The C-character group

It is the object of this chapter to give a somewhat crude description of the group of all the C-characters of a group G. This discussion, however, will be sufficient for determining the order of the C-character group of G, in case G is C-complete.

II. 1. **The automorphisms of a cyclic group.** For the convenience of the reader we collect here a number of known facts concerning the automorphisms of finite cyclic groups([10]).

If E is a cyclic group of order $m\neq 0$, then the group of all the automorphisms of E is a finite abelian group. If g is an automorphism of E, then g determines and is determined by a modulo m uniquely determined number g. Automorphism and number g are related to each other by the fact that the automorphism g of E maps every element in E upon its gth power. A number belongs to an automorphism if, and only if, it is prime to m. This relation between automorphisms and numbers is an isomorphism between the group of automorphisms of E and the multiplicative group of integers prime to m modulo m.

It is sufficient to discuss the case of a primary group E. Then the order of E is a prime power $m=p^{\mu}$.

Case A. *p is odd.* Then the group of all the automorphisms of E is a cyclic group of order $p^{\mu-1}(p-1)$.

Each of the following properties of an automorphism g of E and of the corresponding integer g modulo m implies all the others:

(1) The automorphism g is not of order a power of p.

(2) 1 is the only element in E which is left invariant by g.

(3) The integer g is not congruent to 1 modulo p.

([10]) See, for example, Hecke, op. cit. §13.

It will be convenient to term the automorphisms of order a power of p *regular automorphisms of* E and those meeting the requirements (1) to (3) *irregular automorphisms of* E.

If g is an irregular automorphism of E, then $g-1$ is prime to p and the order n of the automorphism g is the least positive integer k such that $(g^k-1)/(g-1)\equiv 0$ modulo m.

The (regular) automorphism g is of order $p^{\mu-i}$ for $0<j<\mu$ if, and only if, the integer g is congruent to $1+p^ig'$ modulo m for g' an integer prime to p. Then $(g^{p^{\mu-j}}-1)/(g-1)$ is divisible by $p^{\mu-i}$, but not by $p^{\mu-i+1}$.

Case B. $p=2$. If E is of orders 1 or 2, then the identity is the only automorphism of E. Thus we assume that $1<\mu$. Then E contains one and only one element of order 2 and this is left invariant by every automorphism of E.

The automorphism of E which maps every element in E upon its inverse shall be termed the *inversion of* E and shall be denoted by z. The group of all the automorphisms of E is the direct product of a cyclic group of order $2^{\mu-2}$ and of the group of order 2 which is generated by the inversion z.

The following two properties of an automorphism g of E and of the corresponding integer g modulo m are equivalent:

(i) The elements of orders 1 and 2 are the only elements in E which are left invariant by the automorphism g.

(ii) $g\equiv -1$ modulo 4.

We shall term the automorphisms of E meeting the requirements (i), (ii) *irregular automorphisms of* E, the others *regular automorphisms of* E. We note that the inversion is an irregular automorphism.

If the automorphism g of E is different both from the identity and the inversion, then the corresponding integer g is of the form $g\equiv \pm 1+2^ig'$ modulo m where g' is odd and $1<j<\mu$; and the order of the automorphism g is $2^{\mu-i}$.

If g is a regular automorphism of order $2^i\neq 1$, then $(g^{2^i}-1)/(g-1)$ is divisible by 2^i, though not by 2^{i+1}. If g is an irregular automorphism of order 2^i, not the inversion, then $(g^{2^i}-1)/(g-1)$ is divisible by $2^{\mu-1}$, but not by 2^μ.

We extend the definition of a regular automorphism of E, in case E is of orders 1 or 2, by saying that the identity automorphism is always regular.

The classification of automorphisms of E leads naturally to a *classification of the homomorphisms* C.

Suppose that E is a cyclic group of order $m=\prod_p p^{m(p)}$, $E(p)$ the subgroup of prime power order $p^{m(p)}$, that G is a finite group and that C is a homomorphism of G into the group of automorphisms of E. If every element in G induces (under C) in every $E(p)$ a regular automorphism, then C is termed *regular*, otherwise *irregular*. If in particular $1<m(2)$ and an element in G induces the inversion in $E(2)$, then C is said to be *singular* (so that a singular C is always irregular). We note that every G/G_{C_p} is of order a power of p, if C is regular, though this condition is not sufficient for regularity, since G/G_{C2} is always of order a power of 2.

II. 2. **The C-characters of automorphism groups of primary cyclic groups.** In this section we are concerned with a complete determination of the C-characters of a group G which is mapped isomorphically by C upon a group of automorphisms of the cyclic group E of prime power order.

THEOREM II.2.1. *Suppose that C is a non-singular isomorphism of the group G into the group of automorphisms of the cyclic group E of prime power order $m=p^\mu$.*

(a) *Every C-character of G belongs to the principal genus so that the C-character group of G is a cyclic group.*

(b) *If C is regular, then G and its C-character group are of equal order.*

(c′) *If C is irregular and p is odd, then the C-character group of G is of order $m=p^\mu$.*

(c″) *If C is irregular and $p=2$, then the C-character group of G is of order $2^{\mu-1}$.*

Proof. We may assume throughout that $G\neq 1$.

Case A([11]). *p is odd.* Then the group of all the automorphisms of E is a cyclic group. Hence G is a cyclic group, generated by some element g.

Case A′. *C is regular.* Then the integer g corresponding to the automorphism g of E is of the form $g\equiv 1+p^jg'$ modulo m where g' is prime to p and $0<j<\mu$; and the order of g (and of G) is $p^{\mu-j}=n$.

If f is a C-character of G, then $1=f(g^n)=f(g)^s$ where the exponent $s\equiv 1+g+\cdots+g^{n-1}\equiv(g^{p^{\mu-j}}-1)/(g-1)$ is divisible by $p^{\mu-j}$, but by no higher power of p. Consequently $f(g)$ is an element in $E^{p^j}=E^{1-g}$. There exists therefore an element v in E such that $f(g)=v^{1-g}$ and it is readily verified that $f(g^i)=v^{1-g^i}$. Thus every C-character of G belongs to the principal genus; and G and its C-character group are of the same order $p^{\mu-j}$, since the unit character e^{1-x} for e a generator of E is of order $p^{\mu-j}$.

Case A″. *C is irregular.* Then neither G nor g is of order a power of p. Hence $g-1$ is prime to p so that $E=E^{1-g}$. There exists therefore to every C-character f of G an element v in E such that $f(g)=v^{1-g}$; and it is readily seen that $f(g^i)=v^{1-g^i}$. Thus every C-character of G belongs to the principal genus; and the order of the C-character group is m, since e^{1-x} for e a generator of E is of order m.

Case B. $p=2$. G contains just one element of order 2, since G does not contain the inversion of E. Hence G is cyclic (and $2<\mu$). Denote by g some element generating G.

Case B′. *C is regular.* Then $g\equiv 1+2^jg'$ modulo m where g' is odd and $1<j<\mu$; and an exact repetition of the argument used in Case A′ shows that every C-character of G belongs to the principal genus, and that G and its C-character group are of the same order $2^{\mu-j}$.

([11]) These cases refer to the analogous cases in II.1.

Case B''. *C is irregular.* This occurs if, and only if, $g \equiv -1$ modulo 4, that is if, and only if, g is of the form $-1+2^j g'$ where g' is odd and $1<j<\mu$, since g is not the inversion of E. Then $1-g \equiv 2-2^j g' \equiv 2g''$ modulo m where g'' is odd. Hence $E^{1-g}=E^2$ showing that the order of the principal genus is $2^{\mu-1}$. The order of the automorphism g and of the group G is $2^{\mu-j}=n$. Thus every C-character f of G satisfies $1=f(g^n)=f(g)^s$ where the exponent $s=1+g+\cdots+g^{n-1}=(g^{2^{\mu-j}}-1)/(g-1)$ is divisible by $2^{\mu-1}$, but not by 2^μ. From this fact we deduce that $f(g)$ is an element in $E^2=E^{1-g}$; and it follows as usual that f belongs to the principal genus, completing the proof.

THEOREM II.2.2. *Suppose that C is a singular isomorphism of the group G into the group of automorphisms of the cyclic group E of order* $m=2^\mu$.

(a) *The principal genus is of order* $2^{\mu-1}$ *and the C-character group of G is of order* 2^μ.

(b') *If G is cyclic (of order 2), then the C-character group of G is cyclic.*

(b'') *If G is not cyclic, then the C-character group of G is the direct product of the principal genus and of the cyclic group of order 2 which consists of all the C-characters of G mapping the inversion z upon* 1.

Proof. We distinguish two cases.

Case 1. *G is cyclic.* Then G consists of the elements z and $z^2=1$, since z generates a direct factor of the group of all the automorphisms of E. If v is any element in E, then $f(z)=v$ defines a C-character of G because of $f(z)^z f(z)=1$. Hence the order of the C-character group of G is m. If u is the unit character e^{1-z}, then $u(z)=e^{1-z}=e^2$ so that the principal genus is of order $2^{\mu-1}$.

Case 2. *G is not cyclic.* Then there exists a basis of the abelian group G which contains z, and which therefore has the form z, g where g is an element of order $n=2^{\mu-j}$ with $1<j<\mu$.

If f is a C-character of G, then $f(g)^{-1}f(z)=f(g)^z f(z)=f(gz)=f(zg)=f(z)^g f(g)$ or

$$(+) \qquad f(g)^2 = f(z)^{1-g}.$$

Put $v=f(z)$. Then $v^{1-z}=v^2=f(z)^2$ and $v^{1-g}=f(z)^{1-g}=f(g)^2$; and $f(x)^2=v^{1-x}$ is a consequence of the fact that z and g generate G. Thus we have shown that the square of every C-character belongs to the principal genus.

It is a consequence of Theorem II.2.1 that every C-character of the cyclic group generated by g belongs to the principal genus. Hence there exists to every C-character f of G an element v in E such that $f(g)=v^{1-g}$; and we deduce from (+) that $v^{2(1-g)}=f(z)^{1-g}$. Since E is cyclic and g an automorphism, not the identity, this implies that $f(z)$ is in E^2. If w is an element in E such that $f(z)=w^2$, then the C-character $f'(x)=f(x)w^{x-1}$ has the property that $f'(z)=1$; and we have shown that every C-character f of G is modulo the principal genus congruent to a C-character of G which maps z upon 1.

Suppose now that r is a C-character of G such that $r(z)=1$. Then it follows

from (+) that $r(g)^2=1$. If $r(g)=1$, then $r=1$. Since the element of order 2 in E is left invariant by every automorphism of E, there exists one and only one C-character of G (which is at the same time a C_0-character of G) which maps z upon 1 and g upon the element of order 2. Hence the principal genus is of index 2 in the C-character group of G. If the C-character r of G satisfies $r(z)=1\neq r(g)$, then r cannot be in the principal genus, since otherwise there existed an element s in E, satisfying $s^2=s^{1-z}=r(z)=1$ and $s^{1-g}=r(g)\neq 1$, an impossibility since g is odd and $1-g$ is even. Thus we have shown that the C-character group is the direct product of the principal genus and of a cyclic group of order 2. The order of the principal genus is $2^{\mu-1}$, since $E^2=E^{1-z}$; and this completes the proof.

The following statement is an immediate consequence of the two preceding theorems.

COROLLARY II.2.3. *Suppose that C is an isomorphism of the group G into the group of automorphisms of the cyclic group E of prime power order $m=p^\mu$.*

(a) *The C-character group of G is cyclic if, and only if, G is cyclic.*

(b) *The C-character group of G is equal to the principal genus if, and only if, C is not singular.*

We conclude this section with a proof of the following fact.

COROLLARY II.2.4. *Suppose that C is an isomorphism of the group G into the group of automorphisms of the cyclic group E of prime power order $m=p^\mu$. Then the C-character f of G belongs to the principal genus if, and only if, one of the following conditions is satisfied:*

(1) *4 does not divide m;*

(2) *4 is a divisor of m, but none of the elements in G induces in E the inversion z;*

(3) *4 is a divisor of m, the group G contains an element z which induces in E the inversion z and $f(z)$ is in E^2, $f(g)=f(z)^{(1-g)2^{-1}}$ for every g in G.*

Proof. It is an immediate consequence of Corollary II.2.3(b) that every C-character of G is a principal character, if condition (1) or (2) is satisfied. Thus we assume now that neither (1) nor (2) be satisfied by G and C. If (3) is satisfied by the C-character f, then there exists an element v in E such that $f(z)=v^2$; and $f(g)=f(z)^{(1-g)2^{-1}}=v^{1-g}$ for every g in G is a principal character. If conversely f is a principal character, then there exists an element e in E such that $f(x)=e^{1-x}$ for every x in G. In particular $f(z)=e^{1-z}=e^2$ is in E^2 and $f(g)=e^{1-g}=f(z)^{(1-g)2^{-1}}$, since g is odd and $1-g$ is even.

II.3. **The principal genus.** It is obvious that C-characters in the principal genus map G_C upon 1. The problem to be discussed in this section is therefore that of characterizing the principal genus among the C-characters mapping G_C upon 1. We use the following *notations*:

(II.3.*) E is a cyclic group of order $m=\prod_p p^{m(p)}$, $E(p)$ the cyclic subgroup

of prime power order $p^{m(p)}$ of E; G is a group and C a homomorphism of G into the group of automorphisms of E.

THEOREM II.3.1. *The C-character f of G belongs to the principal genus if, and only if, the following conditions are satisfied by f:*

(1) *if the automorphism induced by the element g in G leaves every element in $E(p)$ invariant, then the order of $f(g)$ is prime to p;*

(2) *if 4 is a divisor of m, and if the element z in G induces the inversion in $E(2)$, then $f(z)$ belongs to E^2 and $f(g)^{m2^{-m(2)}} = f(z)^{(1-g)m2^{-m(2)-1}}$ for every g in G.*

Proof. If f is any C-character of G, then $f^{mp^{-m(p)}} = f_p$ is a Cp-character of G. If f is a principal character, then there exists an element v_p in $E(p)$ such that $f_p(x) = v_p^{1-x}$ is a principal Cp-character of G. Consequently $f_p(x) = 1$ for x in G_{Cp}, or equivalently, the order of $f(x)$ is prime to p for x in G_{Cp}. But x is in G_{Cp} if, and only if, the automorphism induced by x leaves every element in $E(p)$ invariant, showing the necessity of (1). The necessity of (2) is an immediate consequence of Corollary II.2.4 (3). If conversely conditions (1), (2) are satisfied by f, then we infer from (1) that f_p maps G_{Cp} upon 1; and hence it follows from (2) and Corollary II.2.4 (3) that f_p is a principal Cp-character of G. Thus there exists, for every prime p, an element v_p in $E(p)$ such that $f_p(x) = v_p^{1-x}$ for every x in G. Since $mp^{-m(p)}$ is prime to p, there exists an integer $i(p)$ such that $mp^{-m(p)}i(p) \equiv 1$ modulo $p^{m(p)}$. Put $v = \prod_p v_p^{i(p)}$. Then it is readily seen that $f(x) = v^{1-x}$ for every x in G, showing the sufficiency of the conditions (1), (2).

In the enunciation of the next theorem we make use of the fundamental subgroups $H(p)$, introduced in I.2. We note that $H(p)$ is exactly the set of all the elements in G which are mapped upon 1 by every Cp-character of G; and that $H(p) \leqq G_{Cp}$ by Lemma I.2.3.

THEOREM II.3.2([12]). *The principal genus consists of all the C-characters of G which map G_C upon 1 if, and only if,*

(1) *$H(p)G_C = G_{Cp}$ for every p, and*

(2) *C is not singular.*

REMARK. If E is of prime power order, and if G is C-complete, then condition (1) is automatically satisfied.

Proof. It has been pointed out before that $H(p) \leqq H(p)\, G_C \leqq G_{Cp}$; and it follows from the very definition of $H(p)$ that $G/H(p)$ is a Cp-complete group. Thus it follows from Theorem I.3.1 that $G_{Cp}/H(p)$ is an abelian group the orders of whose elements are divisors of $p^{m(p)}$, and that every C_0-character of $G_{Cp}/H(p)$ is induced by a Cp-character of $G/H(p)$. We note furthermore the obvious fact that every Cp-character of $G/H(p)$ is induced by one and only one Cp-character of G, since Cp-characters of G map $H(p)$ upon 1.

([12]) Corollary III.2.3 below improves upon this theorem.

If $H(p)G_C < G_{Cp}$, then it follows from Theorem I.1.4 that there exists a C_0-character of $G_{Cp}/H(p)$ which maps $H(p)G_C$ upon 1, though it does not map every element in G_{Cp} upon 1; and consequently there would exist a Cp-character of G which does not map G_{Cp} upon 1, though it maps $H(p)G_C$ upon 1. It is obvious that such a C-character maps G_C upon 1 without belonging to the principal genus, proving the necessity of (1).

If $1 < m(2)$, and if there exists in G an element z inducing the inversion in $E(2)$, then we infer from Corollary II.2.3 (b) the existence of a $C2$-character of G which maps G_{C2} upon 1 and which does not belong to the principal genus, proving the necessity of (2).

Suppose conversely that conditions (1), (2) are satisfied by G; and that the C-character f of G maps G_C upon 1. Clearly f is the product of uniquely determined Cp-characters f_p, since a C-character is a Cp-character if, and only if, its order is a power of p. Since f_p is a suitable power of f, it follows that f_p maps G_C upon 1. Since $H(p)$ is mapped upon 1 by every Cp-character of G, we infer from (1) that G_{Cp} is mapped upon 1 by f_p. Now it follows from (2) and Corollary II.2.3(b) that every f_p belongs to the principal genus, showing that the product f of the f_p belongs to the principal genus too. The conditions (1), (2) are therefore sufficient.

COROLLARY II.3.3. *The principal genus consists of all the C-characters of G which map G_C upon* 1, *if the following two conditions are satisfied*:

(1) *if the automorphism g corresponding to the element g in G leaves the elements in $E(p)$ invariant, then its order is prime to p*;

(2) *C is not singular.*

Proof. Suppose that g is an element in G_{Cp}. Then it follows from (1) that its order modulo G_C is prime to p. Consequently $g = g'g''$ where the order of g' is prime to p, the order of g'' is a power of p, and where g'' belongs to G_C. Since g' is an element in G_{Cp} whose order is prime to p, and since Cp-characters of G induce C_0-characters in G_{Cp}, it follows that g' belongs to $H(p)$; and g belongs therefore to $H(p)G_C$, proving that $G_{Cp} = H(p)G_C$. Our contention is now an immediate consequence of Theorem II.3.2.

II.4. **Imbedding of C-complete groups into direct products.** It will be well to remember that C-complete groups may be characterized in two equivalent ways: a group G is C-complete if 1 is the only element mapped upon 1 by every C-character of G; and this is the case if, and only if, 1 is the cross-cut of the subgroups $H(p)$.

The following concepts will prove convenient for the enunciation of our imbedding theorem: suppose that $E(p)$ is a cyclic group of order $p^{m(p)}$ and that C_p is a homomorphism of the group G_p into the group of automorphisms of $E(p)$, where the primes p range over all the prime divisors of some integer m. We form the direct product E of the $E(p)$, the direct product G^* of

the groups G_p and we define the homomorphism C^* of G^* into the group of automorphisms of E as follows: if $\prod_p g_p$ for g_p in G_p is an element in G^*, then the automorphism of E corresponding under C^* to this element induces in $E(p)$ the same automorphism as the automorphism corresponding under C_p to g_p. This homomorphism C^* will always be referred to as *the direct product of the homomorphisms* C_p.

THEOREM II.4.1. *If C is a homomorphism of the group G into the group of automorphisms of E, and if G is C-complete, then G may be imbedded into the direct product of the quotient groups $G/H(p)$ in such a way that the direct product of the homomorphism Cp induces C in G.*

Proof. The homomorphism Cp of G into the group of automorphisms of $E(p)$ is well defined on $G_p = G/H(p)$, since $H(p) \leqq G_{Cp}$ by Lemma I.2.3. We denote by G^* the direct product of the groups G_p and by C^* the homomorphism of G^* into the group of automorphisms of E which we defined as the direct product of the homomorphisms Cp.

If g is an element in G, then put $g^* = \prod_p H(p)g$ an element in G^*; and it is readily seen that a homomorphism of G upon a subgroup of G^* is defined by mapping g upon g^*. If $g^* = 1$, then g is contained in every $H(p)$ and $g = 1$ is a consequence of the C-completeness of G. Thus G has been mapped isomorphically upon a subgroup of G^*. The automorphism of E corresponding under C^* to g^* induces in $E(p)$ the same automorphism which corresponds to g under Cp, that is the automorphism of E corresponding to g^* under C^* is the same as the automorphism of E which corresponds to g under C; and this completes the proof.

If we denote by $h(p)$ *the index of* $H(p)$ *in* G, that is the order of $G/H(p)$, then the following statement is an immediate consequence of Theorem II.4.1.

COROLLARY II.4.2. *If G is C-complete, then the l.c.m. of the $h(p)$ is a divisor of the order of G; and the order of G is a divisor of the product of the $h(p)$.*

We have introduced *the cross-cut* $\overline{H}(p)$ *of all the* $H(q)$ for $q \neq p$; this subgroup $\overline{H}(p)$ consists exactly of those elements in G which are mapped upon elements in $E(p)$ by every C-character of G. If G is C-complete, then the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1 so that a coset of $G/H(p)$ contains at most one element in $\overline{H}(p)$.

THEOREM II.4.3. *If G is C-complete, then each of the following properties implies all the others:*

(1) *G is (essentially) the direct product of the $G/H(p)$.*

(2) *The order of G is $\prod_p h(p)$.*

(3) *Every coset of $G/H(p)$ contains an element in $\overline{H}(p)$.*

(4) *G is the direct product of the $\overline{H}(p)$; and $H(p)$ is the direct product of the $\overline{H}(q)$ for $q \neq p$.*

Proof. The equivalence of (1) and (2) is an obvious inference from Corollary II.4.2 (and Theorem II.4.1). To prove the equivalence of (1) and (3) we consider the map of G into the direct product G^* of the quotient groups $G/H(p)$ which we used in the proof of Theorem II.4.1. Clearly G is the direct product of the $G/H(p)$ if, and only if, G is mapped by this transformation upon the whole group G^*; and this is the case if, and only if, the following condition is satisfied:

(3′) If $C(p)$ is, for every prime p, a coset of $G/H(p)$, then the cross-cut of the sets $C(p)$ is not empty.

Suppose now that (3′) is satisfied; and that, for some given p, $U(p)$ is a coset of $G/H(p)$. Put $U(q)=H(q)$ for $q\neq p$. Then there exists by (3′) an element u contained in all these $U(r)$. Clearly u is in $\overline{H}(p)$, proving that (3) is a consequence of (3′) and therefore of (1).

Suppose conversely that (3) is satisfied, and that $C(p)$ is for every prime p (dividing m) a coset of $G/H(p)$. There exists by (3) to every p an element $c(p)$ in the cross-cut of $C(p)$ and $\overline{H}(p)$. Put $c=\prod_p c(p)$ (the order of the factors does not matter). If p is some prime, then $c\equiv c(p)$ modulo $H(p)$, since $c(q)$ for $q\neq p$ belongs to $\overline{H}(q)\leqq H(p)$; and this shows that c is an element in the cross-cut of the $C(p)$. Thus (3′) is a consequence of (3); and (3) implies (1), since (3′) implies (1).

If G is the direct product of the $\overline{H}(p)$, then it is clear that $H(p)$ is the direct product of the $\overline{H}(q)$ for $q\neq p$, and that G is, for every p, the direct product of $H(p)$ and $\overline{H}(p)$. But this last fact shows that (3) is a consequence of (4). If conversely (3) is satisfied by G, then G is the direct product of $H(p)$ and $\overline{H}(p)$, since in C-complete groups the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1. Thus $\overline{H}(p)$ is of order $h(p)$ and the product of the subgroups $\overline{H}(p)$ is their direct product and is of order $\prod_p h(p)$, showing that G is, by Corollary II.4.2, the direct product of the $\overline{H}(p)$. Hence (3) and (4) are equivalent.

COROLLARY II.4.4. *If G is C-complete, and if $h(p)$ and $h(q)$ are relatively prime for $p\neq q$, then G is the direct product of the $G/H(p)$.*

REMARK. This criterion is satisfied, for example, whenever $h(p)$ is, for every p, a power of p.

Proof. If $h(p)$ and $h(q)$ are relatively prime for $p\neq q$, then the l.c.m. of the $h(p)$ is equal to their product. Hence we deduce from Corollary II.4.2 that $\prod_p h(p)$ is the order of G. Consequently we may infer from Theorem II.4.3 that G is the direct product of the $G/H(p)$.

II.5. **The order of the C-character group.** Noting that $H(p)\leqq G_{Cp}$ by Lemma I.2.3, we may decompose the index $h(p)$ into the product $h'(p)h''(p)$ of two indices where

$h'(p)=$*index of* $H(p)$ *in* G_{Cp}; and

$h''(p)=$*index of* G_{Cp} *in* G.

Furthermore *we define an invariant* $h'''(p)$ as follows:

$h'''(p)=h''(p)$, *if* Cp *is regular.*

$h'''(p)=p^{m(p)}$, *if* p *is odd and* Cp *is irregular.*

$h'''(2)=2^{m(2)}$, *if* $C2$ *is singular.*

$h'''(2)=2^{m(2)-1}$, *if* $C2$ *is neither regular nor singular.*

The motivation for this definition of $h'''(p)$ will be found in Theorems II.2.1 and II.2.2.

LEMMA II.5.1. *$h'(p)$ is a power of p, and $h''(p)\leqq h'''(p)$.*

Proof. Considering that, by the definition of $H(p)$, the group $G/H(p)$ is Cp-complete, it follows from Theorem I.3.1 that $h'(p)$ is a power of p. Since G/G_{Cp} is essentially a group of automorphisms of the cyclic group $E(p)$ of order $p^{m(p)}$, it follows that $h''(p)$ is a divisor of $p^{m(p)-1}(p-1)$, which makes $h''(p)\leqq h'''(p)$ evident.

THEOREM II.5.2[13]. *The order of the C-character group of G is $\prod_p h'(p)h'''(p)$.*

REMARK. If in particular E is of order a power of p, and if G is C-complete, then the order of the C-character group of G is $h'''(p)$ times the order of G_C.

Proof. Denote by $K(p)$ the group of those Cp-characters of G which map G_{Cp} upon 1. Then the order of $K(p)$ is, by Theorems II.2.1 and II.2.2, exactly $h'''(p)$, since every Cp-character of G/G_{Cp} is induced by one and only one Cp-character of G which maps G_{Cp} upon 1. It is a consequence of Theorem I.1.3 that the group of characters of $G_{Cp}/H(p)$ in $E(p)$ is exactly of order $h'(p)$. From Theorem I.3.1 we deduce that every character of $G_{Cp}/H(p)$ in $E(p)$ is induced by one, and therefore by $h'''(p)$, Cp-character of G, since $G/H(p)$ is Cp-complete. The group of Cp-characters of G is therefore of order $h'(p)h'''(p)$. But the C-character group of G is the direct product of the Cp-character groups of G, showing that its order is $\prod_p h'(p)h'''(p)$.

COROLLARY II.5.3. *Suppose that G is C-complete.*

(a) *The order of G does not exceed the order of the C-character group of G.*

(b) *G and its C-character group are of equal order if, and only if, C is regular.*

REMARK. If C is regular, then every $h''(p)$ is a power of p. Hence $h(p)$ is a power of p too, from Lemma II.5.1. Consequently we may deduce from Corollary II.4.4 that G is the direct product of the quotient groups $G/H(p)$.

Proof. It is a consequence of Corollary II.4.2 and of the C-completeness of G that the order of G is a divisor of $\prod_p h(p)$. We infer from Lemma II.5.1 that $h(p)\leqq h'(p)h'''(p)$. Hence (a) is a consequence of Theorem II.5.2.

---

[13] It may be deduced from Theorem III.2.2 (a) and Corollary III.3.2 below that $\prod_p h'(p)$ equals the order of G_C multiplied by $\prod_p h''''(p)$ where $h''''(p)$ is the index of $G_C H(p)$ in G_{Cp}.

If G and its C-character group are of equal order, then we deduce from (a) and Lemma II.5.1 that $h''(p)=h'''(p)$. This equality implies the regularity of C, as follows immediately from the definition of $h'''(p)$. If conversely C is regular, then we infer from Corollary II.4.4 and Theorem II.4.3 that $\prod_p h(p)$ is the order of G; and from the definition of $h'''(p)$ we infer that $h''(p)=h'''(p)$. Hence G and its C-character group are by Theorem II.5.2 of equal order, if C is regular.

Chapter III. Characterization of C-complete groups

III.1. **The case of primary** E. The following lemma will prove helpful in our discussion.

Lemma III.1.1. *If G is a cyclic group of order n, generated by the element g, if E is a cyclic group of order m, if C is a homomorphism of G into the group of automorphisms of E, and if v is an element in E, then $1=v^{1+g+\cdots+g^{n-1}}$ is a necessary and sufficient condition for the existence of a C-character f of G such that $f(g)=v$.*

Proof. The necessity of the condition is an immediate consequence of $1=f(1)=f(g^n)=f(g)^{1+g+\cdots+g^{n-1}}$. If the condition is satisfied, then a single valued G to E function f is defined by $f(g^i)=v^{1+\cdots+g^{i-1}}$ for $0<i\leqq n$; and this function satisfies $v=f(g)$, $1=f(g^n)=f(1)$. If $0<i,\ j\leqq n$, then there exists a uniquely determined integer $k=0,\ 1$ such that $0<i+j-kn\leqq n$; and we find that $f(g^ig^j)=f(g^{i+j-kn})=v^{1+\cdots+g^i+j-kn-1}=v^{1+\cdots+g^{i+j-1}}$, since, in case $k=1$, we may multiply by $1=v^{(1+\cdots+g^{n-1})g^{i+j-n}}$; and we find that

$$f(g^ig^j)=v^{1+\cdots+g^{i-1}v^{g^i}+\cdots+g^{i+j-1}}=v^{1+\cdots+g^{i-1}v^{(1+\cdots+g^{i-1})g^i}}=f(g^i)f(g^i)^{g^i},$$

as was to be shown.

Theorem III.1.2. *If E is a cyclic group of prime power order $m=p^\mu$, and if C is a homomorphism of the group G into the group of automorphisms of E then the following four conditions are necessary and sufficient for C-completeness of G:*

(i) *G_C is abelian;*

(ii) *the orders of the elements in G_C are divisors of m;*

(iii) *$g^{-1}xg=x^g$ for g in G and x in G_C;*

(iv) *if $p=2$, and if the inversion of E is induced by the element z in G, then $z^2=1$.*

Proof. If G is C-complete, then we may infer conditions (i), (ii) from Theorem I.3.1, condition (iii) from Corollary I.3.2; and the necessity of (iv) may be seen as follows: if the element z in G maps every element in E upon its inverse, and if f is a C-character of G, then $f(z^2)=f(z)^zf(z)=f(z)^{-1}f(z)=1$; and the C-completeness of G implies $z^2=1$.

We suppose now that the conditions (i) to (iv) are satisfied by G, C.

Case I. *G/G_C is cyclic*([14]). Then there exists an element g which generates G modulo G_C. We denote by n' the order of G/G_C which is at the same time the order of g modulo G_C; and we put $g^*=g^{n'}$. If $\{y\}$ denotes the cyclic group, generated by the element y, then $\{g\}_C=\{g^*\}$.

The proof of the following statement will be the most important step.

(+) *There exists a C-character f of $\{g\}$ such that g^* and $f(g^*)$ are of equal order.*

We distinguish several cases.

Case 1. *n' is not a power of p.* Then p is odd, $g-1$ is prime to p; and it follows from (ii) that $x^g=x$ for x in G_C implies $x=1$. Hence it follows from (iii) that $g^*=g^{-1}g^*g=g^{*g}$ and that therefore $g^*=1$. (+) is trivially satisfied.

Case 2. *$p=2$ and g induces the inversion in E.* Then it follows from (iv) that $g^2=1$. Hence either $g^*=g^2=1$ and (+) is obvious; or else $g=g^*$ is an element in G_C; and the existence of the desired C-character which is a C_0-character is a consequence of (ii).

Case 3. *n' is a power of p; and in case $p=2$ the integer g corresponding to the element g under C is congruent to* 1 modulo 4. In this case the integer g is of the form $g\equiv 1+p^jg'$ modulo m where g' is prime to p, $0<j\leqq\mu$, and where

$$p = 2,\ 1 < \mu \quad \text{imply} \quad 1 < j.$$

Then we infer from the remarks in II.1 that $n'=p^{\mu-j}$ and that $1+g+\cdots+g^{n'-1}$ is divisible by $p^{\mu-j}$, but not by $p^{\mu-j+1}$. We note that n' is a divisor of the order n of g so that $n=n'n''$ where both n' and n'' are powers of p, since n'' is the order of the element g^* in G_C and since we may therefore apply (ii) on g^*. Since n' is the order of the automorphism g of E, it follows that $g^{n'}\equiv 1$ modulo m; and thus it follows that $n=n'n''$ is a divisor of $n''(1+g+\cdots+g^{n'-1})\equiv 1+g+\cdots+g^{n-1}$ modulo m. Finally we infer from condition (iii) that $g^*=g^{-1}g^*g=g^{*g}$ or $g\equiv 1+p^jg'\equiv 1$ modulo n'', since n'' is by (ii) a divisor of m; and this shows that n'' is a divisor of p^j, since n'' is a power of p whereas g' is prime to p. Hence $n=n'n''=p^{\mu-j}n''$ is a divisor of $p^\mu=m$.

From the last remark we infer the existence of an element v of order n in E. Since it has been shown that n is a divisor of $1+g+\cdots+g^{n-1}$ it follows that $v^{1+g+\cdots+g^{n-1}}=1$; and we infer from Lemma III.1.1 the existence of a C-character f of $\{g\}$ such that $f(g)=v$. Then $f(g^*)=f(g^{n'})=v^{1+g+\cdots+g^{n'-1}}$ is an element of order $n/n'=n''$, since $1+g+\cdots+g^{n'-1}$ is divisible by $n'=p^{\mu-j}$, but not by $n'p$. Since g^* is of order n'', the C-character f of $\{g\}$ meets all the requirements of (+).

Case 4. $p=2$, $1<\mu$, $g\equiv -1$ modulo 4, $g\not\equiv -1$ modulo m. In this case the integer g is of the form $g\equiv -1+2^jg'$ where g' is odd and $1<j<\mu$. Then we

([14]) A proof of our theorem in Case I may be constructed which makes use of Theorem I.3.5.

infer from the remarks in II.1 that $n'=2^{\mu-j}$ and that $1+g+\cdots+g^{n'-1}$ is divisible by $2^{\mu-1}$, but not by 2^{μ}.

It is a consequence of (ii) and (iii) that $g^*=g^{-1}g^*g=g^{*g}$ or $2-2^jg'$ is divisible by the order n'' of g^*. Since n'' is a power of 2, it follows that $n''=1$ or 2, that is that $g^*=1$ or g^* is of order 2.

If $g^*=1$, then (+) is obvious. If g^* is of order 2, then $n=2n'$, $1+g+\cdots+g^{n-1}\equiv 2(1+g+\cdots+g^{n'-1})$ modulo m, since $g^{n'}\equiv 1$ modulo m. If v is any element of order m in E, then $1=v^{1+g+\cdots+g^{n-1}}$, since $1+g+\cdots+g^{n-1}$ is divisible by 2 $2^{\mu-1}=m$; and it follows from Lemma III.1.1 that there exists a C-character f of $\{g\}$ such that $f(g)=v$. Then $f(g^*)=f(g^{n'})=v^{1+g+\cdots+g^{n'-1}}$ is of order 2, since the exponent is divisible by $2^{\mu-1}$, but not by 2^{μ}; and this shows that f meets all the requirements of (+).

Thus we have completed the proof of (+).

Suppose now that f_0 is a C_0-character of G_C in E. Then it follows from (+) that there exists a C-character f_1 of $\{g\}$ which coincides with f_0 on the cross-cut $\{g^*\}$ of G_C and $\{g\}$. Hence we may infer from Lemma I.3.4 the existence of a C-character f of G which induces f_0 in G_C and f_1 in $\{g\}$, since $G=G_C\{g\}$, and since the conditions (i) to (iii) are satisfied by G and C. This shows that every C_0-character of G_C in E is induced by a C-character of G. But this implies C-completeness of G, as follows from Theorem I.3.1, since (i), (ii) are satisfied by G and C.

Case II. *G/G_C is not cyclic.* In this case $p=2$; and G/G_C is the direct product of a cyclic group V by a cyclic group Z of order 2 such that the element of order 2 in Z maps every element in E upon its inverse (note that $2<\mu$). We denote by W the uniquely determined group between G_C and G which satisfies $W/G_C=V$; and we infer from what has been shown in Case I that W is C-complete.

If z is any element, representing the coset of order 2 in Z, then it follows from condition (iv) that z is of order 2. We note finally the obvious fact $G=W\{z\}$.

The proof of the following statement will be the most important step.

(++) *Every C-character of W is induced by a C-character of G.*

Mapping every element g in W upon the element zgz effects an automorphism of W; and g and zgz clearly induce the same automorphism of E. Hence it follows from Lemma I.2.2 that $f_1(x)=f(zxz)$ is a C-character of W whenever f is a C-character of W.

Suppose now that f is any C-character of W. Then it follows from the last remark that $f_2(x)=f(x)f_1(x)=f(x)f(zxz)$ is a C-character of W. If y is any element in G_C, then it follows from (iii) that $zyz=y^{-1}$; and since C-characters of W induce C_0-characters of G_C, we find that $f_2(y)=1$ for y in $G_C=W_C$. Since none of the automorphisms of E which are induced by elements in W maps every element in E upon its inverse, we may apply Theorem II.2.1 upon

f_2. Hence f_2 belongs to the principal genus of W, that is there exists an element v in E such that $v^{1-x}=f_2(x)=f(x)f(zxz)$ for x in W.

Since W is a normal subgroup of G, and since z is an element of order 2, generating G modulo W, it is possible to represent every element in G in one and only one way in the form $g=w(g)z^{i(g)}$ for $w(g)$ in W and $0\leqq i(g)\leqq 1$. Consequently a single-valued G to E function is defined by

$$f'(g) = f(w(g))^{(-1)^{i(g)}}v^{i(g)}$$

where v is the element in E introduced before.

The element g is in W if, and only if, $i(g)=0$ and $g=w(g)$, proving that f and f' coincide on W. If g and y are elements in G, then $gy=w(g)z^{i(g)}w(y)z^{i(y)}$ $=w(g)z^{i(g)}w(y)z^{i(g)}z^{i(g)+i(y)}$. Thus $w(gy)=w(g)z^{i(g)}w(y)z^{i(g)}$ and $i(gy)\equiv i(g)$ $+i(y)$ modulo 2, since W is a normal subgroup of G. From the choice of the element v it follows that $f(z^ixz^i)=v^{1-x^i}f(x)^{(-1)^i}$ for x in W and $i=0$, 1. This implies that

$$\begin{aligned} f[w(gy)] &= f[w(g)]^{w(y)}f[z^{i(g)}w(y)z^{i(g)}] \\ &= f[w(g)]^{w(y)}f[w(y)]^{(-1)^{i(g)}v^{1-w(y)^{i(g)}}}. \end{aligned}$$

One verifies furthermore by substituting the possible values for $i(g)$ and $i(y)$ that

$$[1 - w(y)^{i(g)}](-1)^{i(g)+i(y)} + i(gy) = i(y) + i(g)w(y)(-1)^{i(y)}.$$

Consequently we have finally

$$\begin{aligned} f'(gy) &= f[w(gy)]^{(-1)^{i(gy)}v^{i(gy)}} \\ &= f[w(g)]^{w(y)(-1)^{i(g)+i(y)}}f[w(y)]^{(-1)^{i(y)}v^{i(y)+i(g)w(y)(-1)^{i(y)}}} \\ &= \{f[w(g)]^{(-1)^{i(g)}v^{i(g)}}\}^{w(y)(-1)^{i(y)}}f[w(y)]^{(-1)^{i(y)}v^{i(y)}} \\ &= f'(g)^yf'(y). \end{aligned}$$

Thus f' has been shown to be a C-character of G which induces f in W; and this completes the proof of $(++)$.

Since W is C-complete and contains $G_C=W_C$, it follows from Theorem I.3.1 that every C_0-character of G_C in E is induced by a C-character of W; and hence we infer from $(++)$ that every C_0-character of G_C in E is induced by a C-character of G. The C-completeness of G is now an immediate inference of Theorem I.3.1 and conditions (i), (ii); and this completes the proof of the theorem.

We note that we have proved the following statement:

COROLLARY III.1.3. *If E is a cyclic group of order $m=2^\mu$, $1<\mu$, if C is a homomorphism of the group G into the group of automorphisms of E such that some elements in G are mapped by C upon the inversion of E, if G is C-complete*

(satisfies (i) *to* (iv) *of Theorem* III.1.2), *and if the subgroup W of G contains* G_C, *does not contain elements z inducing the inversion in E, though G is generated by adjoining z to W, then every C-character of W is induced by a C-character of G; and if f is a C-character of W, v an element in E, then there exists a C-character of G which induces f in W and maps z upon v if, and only if,* $v^{1-z}=f(x)f(zxz)$ *for x in W.*

III.2. **Determination of the subgroups** $H(p)$. Throughout this section we shall make use of the notations (II.3.*). For the enunciation of the next theorem it will be convenient to introduce the subgroup $H_1(p)=(G_{Cp})^{p^{m(p)}}(G_{Cp})'$ where X' is the commutator subgroup of the group X. Clearly $H_1(p)$ is the smallest subgroup of G_{Cp} such that $G_{Cp}/H_1(p)$ is an abelian group the orders of whose elements are divisors of $p^{m(p)}$ and $H_1(p)$ is a normal subgroup of G.

THEOREM III.2.1. (a) $H_1(p)\leqq H(p)\leqq G_{Cp}$.

(b) *If Cp is not singular, then* $H(p)/H_1(p)$ *is generated by the elements* $g^{-1}xgx^{-g}$ *for g in* $G/H_1(p)$ *and x in* $G_{Cp}/H_1(p)$.

(c) *If C2 is singular, then* $H(2)/H_1(2)$ *is generated by the elements* $g^{-1}xgx^{-g}$ *for g in* $G/H_1(2)$, *x in* $G_{C2}/H_1(2)$ *and by the squares of those elements in* $G/H_1(2)$ *which induce the inversion in* $E(2)$.

Proof. It is a consequence of the definition of $H(p)$ that $G/H(p)$ is Cp-complete. We infer $H(p)\leqq G_{Cp}$ from Lemma I.2.3; and we deduce from Theorem III.1.2 the validity of the following conditions:

(1) $G_{Cp}/H(p)$ is an abelian group the orders of whose elements are divisors of $p^{m(p)}$.

(2) $g^{-1}xg=x^g$ for g in $G/H(p)$ and x in $G_{Cp}/H(p)$.

(3) $z^2=1$, if $C2$ is singular, and if the element z in $G/H(2)$ induces the inversion in $E(2)$.

Condition (1) implies $H_1(p)\leqq H(p)$.

Now we define the subgroup $H_2(p)$ between $H_1(p)$ and $H(p)$ as follows: If Cp is not singular, then $H_2(p)/H_1(p)$ is generated by the elements $g^{-1}xgx^{-g}$ for g in $G/H_1(p)$ and x in $G_{Cp}/H_1(p)$. If, however, $C2$ is singular, then $H_2(2)/H_1(2)$ is generated by the elements $g^{-1}xgx^{-g}$ for g in $G/H_1(2)$, x in $G_{C2}/H_1(2)$ and by the squares of those elements in $G/H_1(2)$ which induce the inversion in $E(2)$. From conditions (2) and (3) it is immediately deduced that $H_2(p)\leqq H(p)$.

It is an immediate consequence of the definition of the subgroup $H_2(p)$ and of Theorem III.1.2 that the group $G/H_2(p)$ is Cp-complete. Thus it follows from Lemma I.3.3 that $H(p)\leqq H_2(p)$, proving the desired equality of $H(p)$ and $H_2(p)$.

We denote by $p^{J(p)}$ *the order of the subgroup of all those elements in* $E(p)$ *which are left invariant by every automorphism of* $E(p)$ *that is induced by an element in G.* Thus the integer corresponding to the element g in G under Cp

is of the form $g \equiv 1 + p^{J(p)} g_0$ modulo $p^{m(p)}$ for g_0 a suitable integer. From the facts enumerated in II.1 one readily deduces the following two statements:

$J(p) = 0$ if, and only if, $m(p) = 0$ or G/G_{Cp} is not of order a power of p.

$1 \leqq J(2)$ whenever $1 \leqq m(2)$.

For the investigations concerning the principal genus it is important to determine the subgroup $H^*(p)$ *of all those elements in* G *which are mapped upon* 1 *by all the* Cp*-characters of* G *mapping* G_C *upon* 1.

LEMMA III.2.2. (a) $H^*(p) = H(p)G_C$.

(b) *If* Cp *is not singular, then* $H^*(p)/G_C = (G_{Cp}/G_C)^{p^{J(p)}}$.

(c) *If* $C2$ *is singular, then* $H^*(2)/G_C$ *is generated by the elements in* $(G_{C2}/G_C)^2$ *and by the squares of those elements in* G/G_C *which induce the inversion in* $E(2)$.

We note that $J(2) = 1$, if $C2$ is singular.

Proof. It is an immediate consequence of the definition of $H^*(p)$ that $H(p)G_C \leqq H^*(p)$. Since G_C is mapped upon 1 by the principal genus, and since there exists to every element not in G_{Cp} a principal Cp-character which does not map it upon 1, it follows that $H^*(p) \leqq G_{Cp}$. If w is an element in G_{Cp}, though not in $H(p)G_C$, then we infer from the Cp-completeness of $G/H(p)$ and from Theorems I.3.1 and I.1.4 the existence of a Cp-character of G which maps $H(p)G_C$ upon 1, though it does not map w upon 1. Thus w cannot belong to $H^*(p)$ and hence $H^*(p) = H(p)G_C$.

G/G_C is essentially a group of automorphisms of a cyclic group. Hence G/G_C is an abelian group. It is an immediate consequence of the definition of $H^*(p)$ that $G/H^*(p)$ is Cp-complete; and thus it follows from Theorem III.1.2 that

(1) the orders of the elements in the abelian group $G_{Cp}/H^*(p)$ are divisors of $p^{m(p)}$,

(2) $x = g^{-1}xg = x^g$ for x in $G_{Cp}/H^*(p)$ and g in $G/H^*(p)$,

(3) $z^2 = 1$, if $1 < m(2)$ and if the element z in $G/H^*(2)$ induces the inversion in $E(2)$.

From (2) we infer that the orders of the elements in $G_{Cp}/H^*(p)$ are divisors of $p^{J(p)}$. Thus we define the subgroup $H^{**}(p)$ between G_C and G_{Cp} as follows: If Cp is not singular, then $H^{**}(p)/G_C = (G_{Cp}/G_C)^{p^{J(p)}}$. If $C2$ is singular, then $H^{**}(2)/G_C$ is generated by the squares of elements in G/G_C which induce in $E(2)$ the inversion or the identity. From what has been shown thus far we deduce $H^{**}(p) \leqq H^*(p)$. (The condition (1) may now be discarded, since $J(p) \leqq m(p)$.)

If x is an element in $G_{Cp}/H^{**}(p)$ and g an element in $G/H^{**}(p)$, then it follows from the construction of $H^{**}(p)$ that $G/H^{**}(p)$ is commutative, that the orders of the elements in $G_{Cp}/H^{**}(p)$ are divisors of $p^{J(p)}$, and that therefore $g^{-1}xg = x = x^g$ for x in $G_{Cp}/H^{**}(p)$ and g in $G/H^{**}(p)$. Hence by Theorem III.1.2 we have the Cp-completeness of $G/H^{**}(p)$, proving $H^*(p) = H^{**}(p)$.

THEOREM III.2.3. *The principal genus is exactly the set of the C-characters mapping G_C upon* 1 *if, and only if,*

(1) *C is not singular, and*

(2) $[G_{Cp}:G_C]$ *is prime to p for every prime p such that* $m(p)\neq 0$ *and* G/G_{Cp} *is of order a power of p.*

REMARK. $J(p)\neq 0$ if, and only if, $m(p)\neq 0$ and G/G_{Cp} is of order a power of p, as follows from the remarks in II.1.

Proof. Suppose first that the principal genus contains every C-character mapping G_C upon 1. Then it follows from Theorem II.3.2 that (1) is satisfied by G and that $G_{Cp}=H(p)G_C$. Hence we may deduce from Lemma III.2.2(a) that $G_{Cp}=H^*(p)$, and from Lemma III.2.2(b) that $G_{Cp}/G_C=H^*(p)/G_C=(G_{Cp}/G_C)^{p^{J(p)}}$. Consequently $J(p)\neq 0$ implies that the order of G_{Cp}/G_C is prime to p; and this shows the necessity of condition (2), since $J(p)\neq 0$ if, and only if, $m(p)\neq 0$ and G/G_{Cp} is of order a power of p.

If conversely conditions (1) and (2) are satisfied by G, it follows from Lemma III.2.2(a) and (b) and the above Remark that $(G_CH(p))/G_C=H^*(p)/G_C=(G_{Cp}/G_C)^{p^{J(p)}}=G_{Cp}/G_C$. Thus $G_CH(p)=G_{Cp}$; and we infer from Theorem II.3.2 that the principal genus contains all the C-characters, mapping G_C upon 1.

III.3. **The case of composite** E. We remind the reader of the fact that C-completeness of the group G is equivalent to the property: the cross-cut of all the subgroups $H(p)$ is 1. This latter property implies that the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1, for every p, since $\overline{H}(p)$ is the cross-cut of all the $H(q)$ for $q\neq p$. The importance of the last criterion rests on the fact that $\overline{H}(p)$ consists of the elements mapped into $E(p)$ by every C-character of G.

THEOREM III.3.1. *Each of the following properties implies the others.*

(a) *G is C-complete.*

(b) *H(p) does not contain elements of order p in* G_C[15].

(c) G_C *is abelian and the cross-cut of H(p) and* G_C *consists of the elements of order prime to p in* G_C[15].

Proof. If y is an element of order p in G_C, then y belongs to $\overline{H}(p)$, since C-characters of G induce C_0-characters of G_C in E. If G is C-complete, then the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1 so that elements of order p in G_C cannot be in $H(p)$. If G is not C-complete, then the cross-cut H of the subgroups $H(p)$ is different from 1 and is part of G_C so that there exists an element w of prime order r in H. This element w in G_C belongs to $H(r)$, since it belongs to H; and thus we have shown the equivalence of (a) and (b).

If G is C-complete, then G_C is abelian by Theorem I.3.1 so that G_C is the direct product of groups P and Q where P is of order a power of p and Q of

---

(15) Conditions (b) and (c) are supposed to be valid for every prime p.

order prime to p. It is a consequence of (b) that the cross-cut of $H(p)$ and P is 1; and it is a consequence of Theorem III.2.1 that Q is part of $H(p)$, that is Q is the cross-cut of G_C and $H(p)$. That (b) is a consequence of (c) is obvious; and this completes the proof.

COROLLARY III.3.2. *G is C-complete if, and only if, $H^*(p)$ is, for every prime p, the direct product of $H(p)$ and the p-component of the abelian subgroup G_C.*

Proof. If G is C-complete, then G_C is abelian by Theorem III.3.1(c). If G_C is abelian, then it is the direct product of two subgroups $U(p)$ and $V(p)$ where $U(p)$ consists of the elements of order a power of p in G_C and where $V(p)$ consists of the elements of order prime to p in G_C. Since C-characters of G induce C_0-characters of G_C, it follows that $V(p) \leqq H(p)$. Hence we deduce from Lemma III.2.2(a) that $H^*(p) = H(p)\,U(p)$. If G is C-complete, then it follows from Theorem III.3.1(b) that $H^*(p)$ is the direct product of $H(p)$ and $U(p)$. If conversely $H^*(p)$ is the direct product of $H(p)$ and $U(p)$, then the C-completeness of G is a consequence of Theorem III.3.1(b).

The criteria for C-completeness contained in Theorem III.3.1 and Corollary III.3.2, though sufficient for many applications, are unsatisfactory, since the subgroups $H(p)$, $H^*(p)$ which are defined in terms of C-characters are involved, whereas a satisfactory criterion should involve nothing but structural properties of G and C. We note that Theorem III.3.1(2) is really a family of conditions, namely one for every prime p. To solve our problem it is both sufficient and advantageous to find for every preassigned prime p, a criterion assuring the absence([16]) of elements of order p in the cross-cut of $H(p)$ and G_C. The following concept will be used in the enunciation of such a criterion.

(III.3.*) $Q = Q(p)$ is the set of all the elements in G_{Cp} whose order is prime to p.

THEOREM III.3.3. *If G_C is abelian([17]), and if p is a prime, then the following conditions are necessary and sufficient for the absence([16]) of elements of order p in the cross-cut of $H(p)$ and G_C:*

(1) *$Q(p)$ is a normal subgroup of G and $G_{Cp}/Q(p)$ is an abelian group of order a power of p.*

(2) *If y is an element in G and x an element in G_{Cp} such that $xy^{-1}x^{-1}y$ is of order a power of p, then $(xy^{-1}x^{-1}y)^{p^{m(p)-J(p)}} = 1$; and if furthermore $x^{p^{J(p)}}$ is an element of order a power of p in G_C, then([18]) $y^{-1}xy = x^v$.*

([16]) This is property (b) of Theorem III.3.1, stated for one prime number p only.

([17]) Theorem III.3.1 (c) shows that the commutativity of G_C is necessary for the completeness of the group G.

([18]) Here the exponent y stands for a suitable integer which is modulo $p^{m(p)}$ congruent to the integer corresponding to the element y under Cp. It can be shown, however, that the order of the element x is a divisor of $p^{m(p)}$.

(3) *Suppose that* $p=2$, $1<m(2)$ *and that the element* y *in* G *induces the inversion in* $E(2)$[19].

(3′) *If* y^2 *is an element of order a power of* 2 *in* G_C, *then* $y^2=1$.

(3″) *If* g *is an element in* G *such that the integer corresponding to* g *under* $C2$ *is congruent to* -1 *modulo* 4, *if* x *is an element in* G_{C2} *such that* x, $g^{-1}xgx^{-1}$ *and* $y^{-1}xyx^{-1}$ *are of order a power of* 2, *then*[20] $g^{-1}xgx^{-1}=(y^{-1}xyx^{-1})^{(1-g)2^{-1}}$.

Proof. A. Assume that there are no elements of order p in the cross-cut of $H(p)$ and G_C.

We infer from Lemma I.2.3 that $H(p)\leqq G_{Cp}$; and from the definition of $H(p)$ that $G/H(p)$ is Cp-complete. Thus it follows from Theorem III.1.2 that:

(i) $G_{Cp}/H(p)$ is an abelian group the orders of whose elements are divisors of $p^{m(p)}$;

(ii) $v^{-1}xv=x^v$ for v in $G/H(p)$ and x in $G_{Cp}/H(p)$;

(iii) $z^2=1$ for z an element in $G/H(2)$ inducing the inversion in $E(2)$ provided $p=2$ and $1<m(2)$.

As an abelian group G_C is the direct product of subgroups P and K where P consists of all the elements of order a power of p in G_C and where K consists of all the elements of order prime to p in G_C. Since P and K are characteristic subgroups of G_C, they are normal subgroups of G. We infer from (i) that $K\leqq H(p)$; and from our hypothesis, that the cross-cut of $H(p)$ and P is 1. Hence K is the cross-cut of $H(p)$ and G_C.

From (i) and the commutativity of G/G_C it follows that the commutator subgroup G'_{Cp} of G_{Cp} is part of the cross-cut K of $H(p)$ and G_C. Hence G_{Cp}/K is abelian and is therefore the direct product of groups S and T where S consists of all the elements of order prime to p whereas T consists of all the elements of order a power of p. Denote by S^* the subgroup of G_{Cp} which contains K and satisfies $S=S^*/K$. The orders of the elements in S^* are prime to p, since this holds true for the orders of the elements both in K and in S^*/K, that is $S^*\leqq Q(p)$. If r is an element in $Q(p)$, then its order is prime to p and it is contained in a coset of G_{Cp}/K whose order is prime to p, that is r is in a coset belonging to S; and thus we have shown that $Q(p)=S^*$. Thus $Q(p)$ is a subgroup of G_{Cp}; it is therefore a characteristic subgroup of G_{Cp} and a normal subgroup of G. Since $K\leqq Q(p)$ and G_{Cp}/K is abelian, $G_{Cp}/Q(p)$ is abelian of order a power of p, proving the necessity of condition (1).

If y is any element in G, then we also denote by y some integer that corresponds modulo $p^{m(p)}$ to the element y under Cp. From the definition of $J(p)$ we infer the existence of an integer y_0 such that $y=1+p^{J(p)}y_0$.

If y is an element in G and x an element in G_{Cp}, then we infer from (ii) that

---

[19] This condition is vacuous, if none of the elements in G induces the inversion in $E(2)$.

[20] The exponent $(1-g)2^{-1}$ stands for any suitable integer meeting the obvious requirements; it is a consequence of the first part of condition (2) that the value of $(y^{-1}xyx^{-1})^{(1-g)2^{-1}}$ is independent of the particular choice of $(1-g)2^{-1}$.

$$y^{-1}xyx^{-y} = y^{-1}xyx^{-1}x^{1-y} = y^{-1}xyx^{-1}x^{-p^{J(p)}y_0}$$

is an element in $H(p)$. If both $y^{-1}xyx^{-1}$ and $x^{p^{J(p)}}$ are elements of order a power of p in G_C, then $y^{-1}xyx^{-y}$ is an element of order a power of p in the cross-cut of $H(p)$ and G_C so that $y^{-1}xyx^{-y}=1$, proving the necessity of the second part of condition (2). If we do assume only that $y^{-1}xyx^{-1}$ is an element of order a power of p (in G_C), then we infer from (i) and the above equation that

$$\begin{aligned} 1 &\equiv (y^{-1}xyx^{-y})^{p^{m(p)-J(p)}} \equiv (y^{-1}xyx^{-1}x^{-p^{J(p)}y_0})^{p^{m(p)-J(p)}} \\ &\equiv (y^{-1}xyx^{-1})^{p^{m(p)-J(p)}}x^{-p^{m(p)}y_0} \equiv (y^{-1}xyx^{-1})^{p^{m(p)-J(p)}} \text{ modulo } H(p) \end{aligned}$$

so that $(y^{-1}xyx^{-1})^{p^{m(p)-J(p)}}$ is an element of order a power of p in the cross-cut of $H(p)$ and G_C. But such an element is equal to 1, completing the proof of the necessity of (2).

Suppose now that $p=2$ and $1<m(2)$, that the element y in G induces the inversion in $E(2)$ and that y^2 is an element of order a power of 2 in G_C. Then it follows from (iii) that y^2 is an element of order a power of 2 in the cross-cut of G_C and $H(2)$, that is $y^2=1$, showing the necessity of (3′).

If $p=2$, $1<m(2)$, if y induces the inversion in $E(2)$ and if the integer corresponding to the element g in G under $C2$ is congruent to -1 modulo 4, then $(1-g)2^{-1}$ is an odd integer. If $g^{-1}xgx^{-1}$ and $y^{-1}xyx^{-1}$ for x an element in G_{C2} are elements of order a power of 2 (in G_C), then we infer from the commutativity of $G_{C2}/H(2)$ (see (i)!) that

$$\begin{aligned} g^{-1}xgx^{-1}(y^{-1}xyx^{-1})^{(g-1)2^{-1}} &\equiv g^{-1}xgx^{-g}x^{g-1}(y^{-1}xyxx^{-2})^{(g-1)2^{-1}} \\ &\equiv g^{-1}xgx^{-g}(y^{-1}xyx)^{(g-1)2^{-1}}x^{g-1}x^{-2(g-1)2^{-1}} \\ &\equiv g^{-1}xgx^{-g}(y^{-1}xyx)^{(g-1)2^{-1}} \equiv 1 \text{ modulo } H(2) \end{aligned}$$

by (ii); and thus $g^{-1}xgx^{-1}(y^{-1}xyx^{-1})^{(g-1)2^{-1}}=1$ as an element of order a power of 2 in the cross-cut of $H(2)$ and G_C, proving the necessity of (3″).

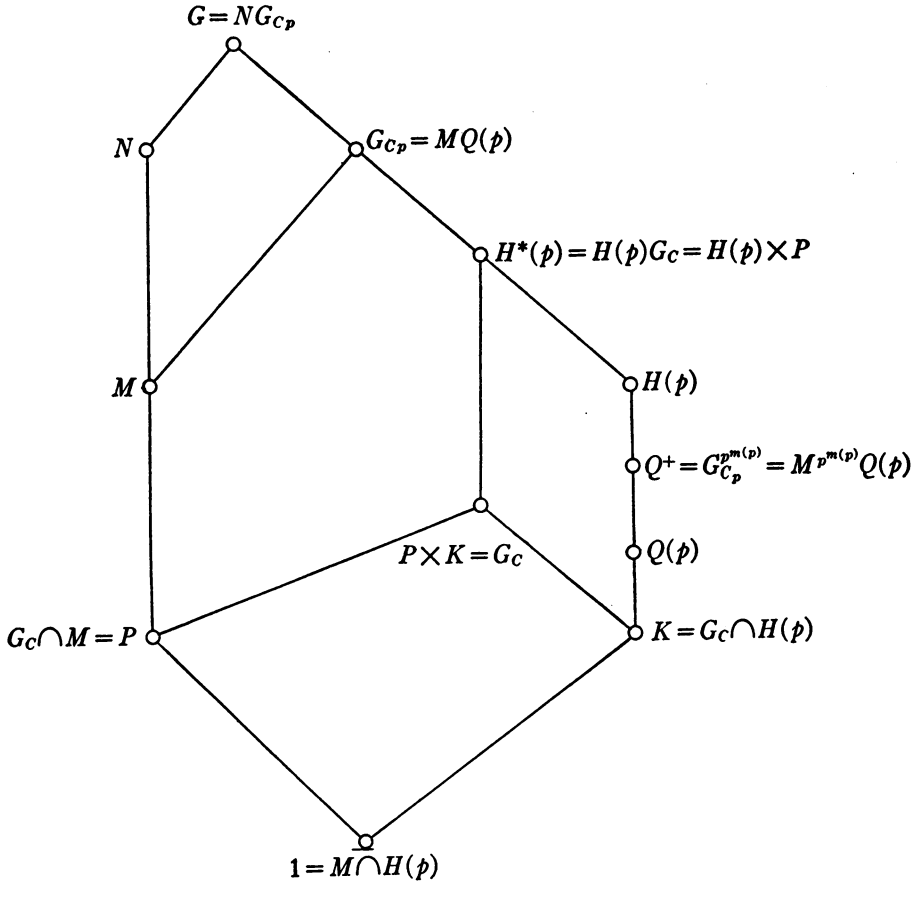
B. Assume that the conditions (1), (2), (3) are satisfied by G, C, p. We distinguish two cases.

B.1. *Cp is not singular.* We select a p-Sylow subgroup M of G_{Cp}. The cross-cut of $Q(p)$ and M is 1; and M contains the subgroup P of all the elements of order a power of p in G_C, since P is a normal subgroup of G. Since any two p-Sylow components of G_{Cp} are conjugate in G_{Cp}, and since every element in G transforms M into another p-Sylow subgroup of G_{Cp}, it follows that every coset of G/G_{Cp} contains elements from the normalizer of M in G. It follows from the special hypothesis B.1 that G/G_{Cp} is a cyclic group; and thus we have shown the existence of an element g in G which generates G modulo G_{Cp} and which transforms M into itself.

It is a consequence of condition (1) that $Q(p)$ is a normal subgroup of G, and that every coset of $G_{Cp}/Q(p)$ contains one and only one element in M.

Thus M and $G_{C_p}/Q(p)$ are isomorphic groups and we infer from (1) the commutativity of M.

If we denote by N the subgroup of G which is generated by adjoining the element g to M, then M is a normal subgroup of N, every coset of N/M is represented by some power of g, and all the elements in the same coset Mg^i of N/M induce in M the same automorphism.



We put $Q^+=Q^+(p)=G_{C_p}^{p^{m(p)}}$. From $Q(p)=Q(p)^{p^{m(p)}}$ and from the commutativity of M (together with the fact that every coset of $G_{C_p}/Q(p)$ contains one and only one element in M) we infer that

$$(') \qquad Q^+ = QM^{p^{m(p)}}.$$

Clearly it follows from (1) that $G_{C_p}/Q^+(p)$ is an abelian group the orders of whose elements are divisors of $p^{m(p)}$. It is readily seen now that $Q^+(p)$ is

exactly the group $H_1(p)$ introduced in Theorem III.2.1; and we infer from this theorem that $H(p)$ is the uniquely determined subgroup of G_{Cp} which contains Q^+ such that $H(p)/Q^+$ is exactly the subgroup of G_{Cp}/Q^+ which is generated by all the elements $v^{-1}wvw^{-v}$ for v in G/Q^+ and w in G_{Cp}/Q^+.

Since G_{Cp}/Q^+ is by (1) an abelian group the orders of whose elements are divisors of $p^{m(p)}$, it follows that every coset V of G/G_{Cp} induces a well-determined automorphism in G_{Cp}/Q^+ which we denote by V also. Thus $v^{-1}wvw^{-v} = w^{V-v}$ for v in G/Q^+, w in G_{Cp}/Q^+ and $V=G_{Cp}v$. From our choice of the element g we infer the existence of an integer i such that $V=G_{Cp}g^i$; and for the integers corresponding under Cp to these elements it follows likewise that $v\equiv g^i$ modulo $p^{m(p)}$. If we put $Z=G_{Cp}g$, then we find for v in G/Q^+ and w in G_{Cp}/Q^+:

$$v^{-1}wvw^{-v} = w^{V-v} = w^{Z^i-g^i} = w^{(Z^{i-1}+Z^{i-2}g+\cdots+Zg^{i-2}+g^{i-1})(Z-g)}.$$

From this equation one readily deduces the following fact:

$$(\prime\prime) \qquad H(p)/Q^+ = (G_{Cp}/Q^+)^{Z-g}.$$

Now let g stand for any integer which modulo $p^{m(p)}$ corresponds under Cp to the element g in G. If x is an element in $H(p)$, then we infer from ($\prime\prime$) the existence of an element Y in G_{Cp}/Q^+ such that $Q^+x=Q^+Y^{Z-g}$. But Y contains an element y in M. Hence it follows from ($\prime$) that x is in

$$Q^+(Q^+y)^{Z-g} = Q^+g^{-1}ygy^{-g} = QM^{p^{m(p)}}g^{-1}ygy^{-g}.$$

Thus we have proved the following statement.

($\prime\prime\prime$) Every element in $H(p)$ has the form:

$$x = x_0x_1^{p^{m(p)}}g^{-1}x_2gx_2^{-g} \qquad \text{for} \quad x_0 \text{ in } Q(p),\ x_1 \text{ and } x_2 \text{ in } M.$$

We note that by the choice of g the element $g^{-1}x_2g$ is in M too so that $x_0^{-1}x$ belongs to M.

Suppose now that x is an element of order a power of p in the cross-cut of $H(p)$ and G_C. Then it follows from ($\prime\prime\prime$) and the remark following ($\prime\prime\prime$) that both x and $x_0^{-1}x$ belong to M, since $P\leqq M$. Hence x_0 is in the cross-cut of $Q(p)$ and M so that $x_0=1$. Since $g^{-1}x_2gx_2^{-1}$ is in the cross-cut P of M and G_C, it follows that $x(g^{-1}x_2gx_2^{-1})^{-1}=x_1^{p^{m(p)}}x_2^{1-g}$ is in P too. (Use the commutativity of M.) From the definition of the integer g and the invariant $J(p)$ we infer the existence of an integer g^* such that $1-g=g^*p^{J(p)}$; and since the element g generates G modulo G_{Cp}, that is the automorphism corresponding to g under Cp generates the group of automorphisms of $E(p)$ induced by elements in G, it follows that g^* is prime to p. Hence

$$(x_1^{p^{m(p)-J(p)}}x_2^{g^*})^{p^{J(p)}} = x_1^{p^{m(p)}}x_2^{1-g}$$

is in G_C and even in P; and it follows from condition (2) (second part) that

$$g^{-1}(x_1^{p^{m(p)-J(p)}g^*}x_2)g = (x_1^{p^{m(p)-J(p)}}x_2^{g^*})^g,$$
$$(g^{-1}x_2gx_2^{-g})^{g^*} = g^{-1}x_2^{g^*}gx_2^{-g^*g} = x_1^{p^{m(p)-J(p)}g}\,g^{-1}x_1^{-p^{m(p)-J(p)}}g;$$

and consequently we find that

$$\begin{aligned} x^{g^*} &= x_1^{g^*p^{m(p)}}(g^{-1}x_2gx_2^{-g})^{g^*} \\ &= x_1^{g^*p^{m(p)}}x_1^{p^{m(p)-J(p)(1-g^*pJ(p))}}(g^{-1}x_1g)^{-p^{m(p)-J(p)}} \\ &= x_1^{p^{m(p)-J(p)}}(g^{-1}x_1^{-1}g)^{p^{m(p)-J(p)}} = (x_1g^{-1}x_1^{-1}g)^{p^{m(p)-J(p)}} \\ &= 1 \end{aligned}$$

as follows from the first part of condition (3). But g^* is prime to p; and hence it follows that $x=1$; and we have shown that the only element of order a power of p in the cross-cut of $H(p)$ and G_C is 1, as we desired to do.

B.2. *$p=2$ and C2 is singular.* Then $J(2)=1$, as has been pointed out before.

We select a 2-Sylow subgroup N of G and denote by M the cross-cut of N and G_{C2}. Since G_{C2} is a normal subgroup of G, it follows that M is a 2-Sylow subgroup of G_{C2}. Since both $G_{C2}/Q(2)$ (by (1)) and G/G_{C2} are of order a power of 2 (see II.1.B), it follows that every coset of $G/Q(2)$ contains one and only one element in N; and we infer from (1) the commutativity of M, as M and $G_{C2}/Q(2)$ are isomorphic.

We denote by Y the set of all the elements in G which induce the inversion in $E(2)$. Clearly Y is a coset of G/G_{C2} and the cross-cut Y^* of Y and N is a coset of N/M.

We denote by $Q^+=Q^+(2)$ the subgroup $G_{C2}^{2^{m(2)}}$; and as in B.1 it follows that $Q^+(2)=Q(2)M^{2^{m(2)}}$ and that $G_{C2}/Q^+(2)$ is an abelian group the orders of whose elements are divisors of $2^{m(2)}$. Then one deduces from Theorem III.2.1 that

(+) $H(2)$ is the uniquely determined subgroup of G_{C2} which contains $Q^+(2)$ such that $H(2)/Q^+(2)$ is generated by the elements y^2 for y in Y and by the elements $v^{-1}wvw^{-v}$ for v in $G/Q^+(2)$ and for w in $G_{C2}/Q^+(2)$.

It will be convenient to start with the investigation of a (possibly smaller) subgroup, namely the subgroup Q^0 between $Q^+(2)$ and $H(2)$ which is uniquely determined by the property that Q^0/Q^+ is generated by the elements y^2 for y in the coset Y of G/G_{C2} [consisting of all the elements in G/Q^+ which induce the inversion in $E(2)$]. Noting that every coset of $G/Q(2)$ contains one and only one element in N and that the inverses of elements in Y belong to Y, it is readily verified that every element x in Q^0 has the form:

$$x = x_0 x_1^{2^{m(2)}} y_1^2 \cdots y_k^2 \qquad \text{for } 0 \leqq k,\ x_0 \text{ in } Q,\ x_1 \text{ in } M,\ y_i \text{ in } Y^*.$$

If $1 < k$, then it is possible to simplify this normal form for elements in Q^0 as follows: Since every y_1 is an element in N which induces the inversion in $E(2)$, all the elements y_i are in the same coset Y^* of N/M; and hence there exist elements z_i in M such that $y_i = z_i y_1$. Since all the elements in Y^* induce in the abelian group M the same automorphism which we denote by Y^*, it follows that $y_i^2 = z_i^{1+Y^*} y_1^2$. Since z_i and y_1^2 are elements in the commutative group M, we deduce that $y_1^2 \cdots y_k^2 = (z_1 \cdots z_k)^{1+Y^*} y_1^{2k}$. Considering that an odd power of an element in Y^* is an element in Y^*, we see finally that every element x in Q^0 has the form:

$$(*) \qquad x = x_0 x_1^{2^{m(2)}} x_2^{1+Y^*} x_3^{2^h}$$

for x_0 in Q, x_1 and x_2 in M, where $x_3 = 1$ if $h = 0$ and x_3 is in Y^* if $0 < h$.

Now we distinguish two cases:

B.2.1. *G/G_{C2} is of order* 2. Then the elements in G induce in $E(2)$ the inversion and the identity; and it follows from (+) and (*) that every element x in $H(2)$ has the form given in (*). Suppose now that such an element x belongs to P (is an element of order a power of 2 in G_C). Since $P \leqq M$, since M is an abelian 2-group, and since $x_0^{-1}x$ and x both belong to M, it follows immediately that $x_0 = 1$. We note furthermore that $x_i^{Y^*-1}$ belongs to the cross-cut P of G_C and M, since it belongs to the commutator subgroup of G which is part of G_C.

If $h = 0$, then $x = x_1^{2^{m(2)}} x_2^{1+Y^*}$ and consequently $(x_1^{2^{m(2)-1}} x_2)^{2^{J(2)}} = x_1^{2^{m(2)}} x_2^2 = x\, x_2^{1-Y^*}$ is an element in P. Hence it follows from the second part of condition (2) that $(x_1^{2^{m(2)-1}} x_2)^{Y^*} = (x_1^{2^{m(2)-1}} x_2)^{-1}$ or $x_2^{Y^*+1} = x_1^{-(Y^*+1)2^{m(2)-1}}$; and thus we find that

$$x = x_1^{2^{m(2)} - (Y^*+1)2^{m(2)-1}} = x_1^{(1-Y^*)2^{m(2)-J(2)}} = 1$$

by the first part of condition (2).

Next if $h = 1$, then

$$x = x_1^{2^{m(2)}} x_2^{1+Y^*} x_3^2 = x_1^{2^{m(2)}} (x_2 x_3)^2 = x_1^{2^{m(2)-1}(1-Y^*)} x_1^{2^{m(2)-1}(1+Y^*)} (x_2 x_3)^2$$
$$= x_1^{2^{m(2)-1}(1-Y^*)} (x_1^{2^{m(2)-1}} x_2 x_3)^2$$

and this shows that $x_1^{2^{m(2)-1}} x_2 x_3$ is an element in Y^* whose square is in P. Thus it follows from condition (3′) that this square is 1 so that $x = x_1^{(1-Y^*)2^{m(2)-J(2)}} = 1$ by condition (2) (first part).

If finally $1 < h$, then $2^{h-1} - 1$ is odd; and we find that

$$x = x_1^{2^{m(2)-1}(1-Y^*)} (x_1^{2^{m(2)-1}} x_2 x_3)^2 x_3^{(2^{h-1}-1)2}.$$

Since both $x_3^{\pm(2^{h-1}-1)}$ and $x_1^{2^{m(2)-1}}x_2x_3$ are elements in Y^*, there exists an element z in M such that $x_1^{2^{m(2)-1}}x_2x_3=zx_3^{1-2^{h-1}}$; and consequently we have $x=x_1^{2^{m(2)-1}(1-Y^*)}z^{1+Y^*}$. The first of the factors is 1 as a consequence of the first part of condition (2); and hence $x=1$ is a consequence of the second part of (2). This completes the proof of the fact that in the case under consideration the cross-cut of P and $H(2)$ is 1.

B.2.2. *G/G_{C2} is not of order* 2. Then we infer from II.1.B and from the existence of elements in G which induce the inversion in $E(2)$ that there exists a basis Z, Y of G/G_{C2} where Y induces the inversion in $E(2)$ and where the integer corresponding to Z under $C2$ is congruent to -1 modulo 4. We note that the cross-cuts Z^* and Y^* of Z and Y respectively with N are cosets of N/M which induce the automorphisms Z^* and Y^* respectively in the commutative group M.

Now one derives from (+) and (*) with the same arguments as were used in B.1 that every element x in $H(2)$ has the form:

$$(**) \qquad x = x_0x_1^{2^{m(2)}}x_2^{1+Y^*}x_3^{Z^*-g}x_4^{2^h}$$

where x_0 is in $Q(2)$, where x_1, x_2 and x_3 are elements in M and x_4 is an element in Y^* if $0<h$, and $x_4=1$ if $0=h$, and where g is an integer which is modulo $2^{m(2)}$ congruent to the integers corresponding under $C2$ to the elements in Z^*.

If x is an element in the cross-cut of $H(2)$ and P, then it follows as usual that $x_0=1$. It follows from condition (3'') and the first part of condition (2) that $x_1^{(1-Y^*)2^{m(2)-1}}=1$ and that $x_3^{(Z^*-g)+(1+Y^*)(g-1)2^{-1}}=1$; and thus we find that

$$x = x_1^{2^{m(2)-1}(1+Y^*)}x_2^{1+Y^*}x_3^{(1+Y^*)(1-g)2^{-1}}x_4^{2^h}.$$

If $x_4^{2^h}=1$, then x is the $(1+Y^*)$th power of some element in M, and $x=1$ is a consequence of the second part of condition (2).

If $h=1$, then $x=v^{1+Y^*}x_4^2=(vx_4)^2$ for v an element in M and vx_4 an element in Y^*; and it follows from condition (3') that $x=1$.

If $1<h$, then $x=v^{1+Y^*}x_4^2x_4^{(2^{h-1}-1)2}=w^{1+Y^*}$ for some element w in M (the existence of w is seen as in case B.2.1) and we infer again from the second part of condition (2) that $x=1$. Thus it follows that the cross-cut of P and $H(2)$ is 1; and this completes the proof of the theorem.

REMARK. From condition (2) one derives readily that $x^{p^{m(p)}}=1$ for every element x in G_{Cp} such that $x^{p^{m(p)}}$ is an element of order a power of p in G_C.

CHAPTER IV. UNIQUENESS OF THE C-CHARACTER GROUP

The group B of C-characters of the group G shall be termed *complete, if* 1 *is the only element in G mapped upon* 1 *by every C-character in B*; and the complete group B of C-characters of G may be called *strictly complete, if B contains the principal genus*. The C-character group of G (that is, the group of

all the C-characters of G) is obviously complete if, and only if, G is C-complete. Thus there arises the problem([21]) of determining conditions assuring that the C-character group of G is the only complete (the only strictly complete) group of C-characters of G; and we devote this chapter to a solution of this problem.

IV.1. **Criteria depending on the nature of the homomorphism C only.** If G is C-complete, then G is by Theorem I.3.1 an extension of the abelian group G_C by the abelian group G/G_C; and the homomorphism C effects an isomorphism of G/G_C into the group of automorphisms of the cyclic group E. The criteria in this section will depend (like the investigations of Chapter II) only on the nature of the isomorphism C of the quotient group G/G_C.

THEOREM IV.1.1. *If the group G is C-complete, if the order of G_{C_p}/G_C is prime to p whenever $0<m(p)$ and G/G_{C_p} is of order a power of p, and if $C2$ is not singular, then the C-character group of G is the only strictly complete group of C-characters of G.*

Proof. If B is a complete group of C-characters of G, then it follows from the C-completeness of G and from Theorems I.3.1 and I.1.4 that every C_0-character of G_C in E is induced by some C-character in B. Thus there exists to every C-character f of G at least one C-character b in B such that f and b coincide on G_C. Since fb^{-1} is a C-character of G which maps G_C upon 1, it follows from our hypotheses and Theorem III.2.3 that fb^{-1} belongs to the principal genus. If B is strictly complete, then fb^{-1} is in B, showing that f itself belongs to B, that is, every strictly complete group B of C-characters of G is the (full) C-character group of G.

THEOREM IV.1.2. *If G is C-complete, if C is regular, then the C-character group of G is the only complete group of C-characters of G.*

Proof. It is an immediate consequence of Corollary II.5.3 and our hypothesis that G and its (full) C-character group are of equal order N. Suppose now that B is a complete group of C-characters of G. Then its order N^* certainly does not exceed N [is a divisor of N].

If g is an element in G, then we define a single-valued B to E function([22]) $F_g(f)$ by the rule $F_g(f)=f(g)$ for every f in B. It is readily verified that F_g is a C_0-character of B in E; and we note that B is an abelian group the orders of whose elements are divisors of the order m of E. The elements x and y in G satisfy $F_x=F_y$ if, and only if, $f(x)=f(y)$ for every f in B; and this is equivalent to

$$1 = [f(x)f(y)^{-1}]^{y^{-1}} = f(x)^{y^{-1}}f(y)^{-y^{-}} = f(x)^{y^{-1}}f(y^{-1}) = f(xy^{-1})$$

([21]) A solution of this problem is important by its applications to the theory of radical extensions of fields, as will be shown elsewhere.

([22]) Cp. V.1 below for a more detailed study of this operator F_g.

for every f in B. Since B is a complete group of C-characters of G, it follows that $F_x = F_y$ if, and only if, $xy^{-1}=1$ or $x=y$. Thus we have shown that the set F_G of all the C_0-characters F_g of B consists of exactly N characters. It is a consequence of Theorem I.1.3 that the order of the group of all the C_0-characters of B in E is exactly N^* showing that $N \leqq N^*$. But we have pointed out before that N^* does not exceed N showing that $N=N^*$, that is, B and the (full) C-character group of G are of equal order and are therefore equal, as was to be shown.

We note that the methods employed in the proofs of the two preceding theorems are completely exhausted by these theorems.

The following lemma will prove useful in the future.

LEMMA IV.1.3. *If G is C-complete, if G^* is a subgroup of G such that $G=G_C G^*$, if B is a group of C-characters of G such that every C-character of G^* is induced by some C-character in B, and if to every element w in G_C whose order modulo*([23]) *G^* is a prime there exists a C-character in B which maps G^* but not w upon 1, then B is the full C-character group of G.*

Proof. If f is a C-character of G, then there exists a C-character b in B such that f and b coincide on G^*. Thus $f_1=fb^{-1}$ is a C-character of G which maps G^* upon 1. If B^* is the group of all the C-characters in B which map G^* upon 1, then it follows from our hypotheses that $G_C{}^*$ is the set of all the elements in G_C which are mapped upon 1 by all the characters in B^*. Hence it follows from Lemma I.3.4 and Theorem I.1.4 that every C_0-character of G_C in E which maps $G_C{}^*$ upon 1 is induced by one and only one C-character in B^*; and thus it follows that the character f_1, constructed above, belongs to B^*. Hence $f=f_1 b$ belongs to B; and this completes the proof.

IV.2. **The case of primary E and cyclic G/G_C.** Throughout this section we impose the following hypotheses([24]):

(IV.2.*) E is a cyclic group of prime power order $m=p^\mu$, C is a homomorphism of the group G into the group of automorphisms of E, and G is C-complete.

These hypotheses imply the cyclicity of G/G_C, if m is odd, but not in the case of even m. Thus we add the following requirement:

(IV.2.**) G/G_C is cyclic.

THEOREM IV.2.1. *The C-character group of G is the only strictly complete group of C-characters of G if, and only if, C is not singular.*

Proof. If the condition of the theorem is satisfied, then the hypotheses of Theorem IV.1.1 are satisfied too, showing the sufficiency of our condition.

([23]) More precisely, modulo the cross-cut of G^* and G_C.

([24]) Without restating them in the hypotheses of the various theorems of this section.

If the condition is not satisfied, then $p=2$, $1<\mu$ and there exists in G an element z inducing the inversion in E. Because of the cyclicity of G/G_C it follows that z generates G modulo G_C; and $z^2=1$ is a consequence of the C-completeness of G, as follows from Theorem III.1.2. We denote by B the group of all those C-characters of G which map z upon an element in E^2. From $v^{1-z}=v^2$ for v in E we infer that B contains the principal genus. From Lemma I.3.4 and $z^2=1$ we deduce that every C_0-character of G_C in E is induced by one and only one C-character of G which maps z upon 1; and this implies that every C_0-character of G_C in E is induced by some C-character in the group B. Hence it follows from the C-completeness of G and Theorems I.3.1 and I.1.4 that there exists to every element $y\neq 1$ in G_C a C-character in B which does not map y upon 1; and if y is an element in G though not in G_C, then y is mapped upon elements different from 1 by the principal genus which is part of B. Thus B is a strictly complete group of C-characters of G. But we infer from Lemma I.3.4 and $z^2=1$ the existence of a C-character of G which maps G_C upon 1 and the element z upon an element not in E^2, that is, B is not the full C-character group of G as was to be shown.

THEOREM IV.2.2. *The C-character group of G is the only complete group of C-characters of G if, and only if, one of the following (mutually exclusive) conditions is satisfied*:

(1) *If p is odd and $G\neq G_C$, then either $m=p$ or the order of G/G_C is divisible by p.*

(2) *If $p=2$, G/G_C of order 2, and if C is irregular, then $G_C^2<G^2$.*

Proof. If $G=G_C$, then the C-characters of G are C_0-characters of G in E; and it follows from Theorem I.1.4 that the character group of G is the only complete group of characters. Consequently we assume in the following that G and G_C are different. This implies in particular that m is neither 1 nor 2.

If C is regular, then we infer from Theorem IV.1.2 that the C-character group of G is the only complete group of C-characters of G. Consequently we assume in the following that C is irregular.

If $p=2$, and if there exists in G an element z inducing the inversion in E, then G/G_C is of order 2, since it is cyclic; and $G^2=G_C^2$, since every element in G, not in G_C, induces the inversion in E, and since it follows from the C-completeness of G and Theorem III.1.2 that $y^2=1$, if y induces the inversion in E. On the other hand we infer from Theorem IV.2.1 that the C-character group of G is not the only complete group of C-characters of G. Consequently we may assume in the following that G does not contain an element inducing the inversion in E, if $p=2$.

Since G/G_C is cyclic, there exists an element g in G which generates G modulo G_C. If p is odd, then the automorphism induced by g in E is not of order a power of p; and we infer from II.1.A that the integer $g-1$ is prime to

p. The automorphism g of E does not leave invariant any element different from 1; and hence it follows from the C-completeness of G and from Theorem III.1.2 that 1 is the only element in G_C permuting with g. This implies in particular that the element g and the automorphism g of E are of equal order n.

If $p=2$, then the integer g corresponding to g under C is of the form $g\equiv -1+2^j g'$ modulo m for g' an odd number and $1<j<\mu$, since the integer corresponding to a square in G cannot be congruent to -1 modulo 4, and since G does not contain an inversion of E. We infer from II.1.B that the automorphism g of E is of order $2^{\mu-j}$. Since the automorphism g of E leaves only the elements in E whose order is a divisor of 2 invariant, it follows from the C-completeness of G and from Theorem III.1.2 that g permutes only with those elements in G_C whose orders are divisors of 2; and this implies in particular that the element $g^*=g^{2^{\mu-j}}$ in G_C is either 1 or of order 2.

We distinguish several cases.

Case 1. *If p is odd, then condition* (1) *is satisfied by G; and if $p=2$, then the order of G/G_C is divisible by* 4. We prove some lemmas.

(1.A) *Every complete group B of C-characters of G contains a character b such that $b(g^i)=1$ implies $g^i=1$.*

The complete group B of C-characters of G induces in the cyclic group $\{g\}$ generated by the element g a complete group $\overline{B}$ of C-characters. If p is odd and $m=p$, then we infer from Theorem II.5.2 that the C-character group of $\{g\}$ is a cyclic group of order p which is clearly generated by every element not 1. Since $\overline{B}$ cannot be 1, there exists in B a character b such that $b(g)\neq 1$ and this character b generates the full C-character group of $\{g\}$ and has therefore the desired qualities. Assume now that $m\neq p$. Then there exists a divisor n' of the order of the automorphism g of E such that $g''=g^{n'}$ is an automorphism of order p of E. It is a consequence of II.1 that the integer corresponding to g'' under C is of the form $g''\equiv 1+p^{\mu-1}g'''$ modulo m for g''' an integer prime to p. There exists in B a character b such that $b(g'')\neq 1$; and if $p=2$, but $g^*\neq 1$, then b may and shall be required to satisfy $b(g^*)\neq 1$. If $p=2$, $g^*=1$, then g'' is the only element of order 2 in $\{g\}$; and if $p=2$, $g^*\neq 1$, then g^* is the only element of order 2 in $\{g\}$; and thus $p=2$ and $b(g^i)=1$ imply that $g^i=1$. If p is odd, then $\{g\}_C=1$, as has been pointed out before; and it is a consequence of Theorem II.3.2 that every C-character of $\{g\}$ belongs to the principal genus. Hence there exists an element v in E such that $b(g^i)=v^{1-g^i}$. Since $1\neq b(g'')=v^{-p^{\mu-1}v'''}$, it follows that v is of order p^μ and that therefore v generates E. If $1=b(g^i)$ for some i, then g^i consequently leaves every element in E invariant; and this implies $g^i=1$, since the element g in G and the automorphism g of E have the same order n.

(1.B) *If the C-character d of* $\{g\}$ *does not map any element except* 1 *upon* 1, *then every C-character of* $\{g\}$ *is a power of d.*

If $m=p$, then the C-character group of $\{g\}$ is by Theorem II.5.2 a cyclic group of order p which is generated by each of its elements excepting 1. If $m\neq p$, and if $g^*=1$ in case $p=2$, then it follows from Theorem II.3.2 that every C-character of $\{g\}$ belongs to the principal genus, that therefore $d(g^i)=v^{1-\vartheta^i}$ for v in E, and that v is an element of order m in E, since $1\neq d(g'')$ for $g''=g^{n'}$ an automorphism of order p of E; and it is readily seen that every C-character of $\{g\}$ is a power of d. (Note that $g''\equiv 1+p^{\mu-1}g'''$ modulo m for g''' an integer prime to p.) If $p=2\neq m$, and if $g^*\neq 1$, then[25] one verifies in the same way that d^2 generates the principal genus of $\{g\}$ and that therefore every C-character of $\{g\}$ is a power of d, since it coincides with d or d^2 on g^*.

Suppose now that B is a complete group of C-characters of the group G. Then we denote by B_0 the group of all those C-characters in B which map g upon 1.

Consider an element w in G_C whose order modulo $\{g\}$ is p. If p is odd then the cross-cut of $\{g\}$ and G_C is 1 so that w is an element of order p in G_C. If $p=2$, then the cross-cut of $\{g\}$ and G_C is either 1 or generated by the element g^* of order 2; thus w is either of order 2 or $w^2=g^*$ and w is of order 4.

It is a consequence of (1.A) that there exists in B a C-character b such that $b(g^i)=1$ implies $g^i=1$; and we deduce from (1.B) that every C-character of $\{g\}$ is induced by some power of b.

If $b(w)=1$, then we deduce from the completeness of B the existence of a C-character f in B such that $f(w)\neq 1$; and there exists (by the remark made in the preceding paragraph) an integer k such that f and b^k coincide on $\{g\}$. Clearly $f_1=fb^{-k}$ belongs to B_0 and satisfies $f_1(w)=f(w)b(w)^{-k}=f(w)\neq 1$, showing that w is not mapped upon 1 by B_0.

If $b(w)\neq 1$, but w is of order p, then $b(w)$ is of order p, since b induces a C_0-character in G_C. There exists an integer r such that $b(g^r)$ is of order p; for if $m=p$ and p is odd, then take $r=1$; if p is odd, but $m\neq p$, then choose r in such a fashion that g^r induces an automorphism of order p in E, and a like choice is appropriate if $p=2$ and $g^*=1$; if $g^*\neq 1$, then $b(g^*)$ is of order 2. Since $b(g^r)$ and $b(w)$ are of equal order p, there exists an integer s, prime to p, such that $b(g^r)=b(w)^s=b(w^s)$; and we have $b(g^rw^{-s})=b(g^r)b(w)^{-s}=1$. From the completeness of B we infer the existence of a C-character f_2 in B such that $f_2(g^rw^{-s})\neq 1$; and there exists an integer k' such that f_2 and $b^{k'}$ coincide on $\{g\}$. Clearly $f_3=f_2b^{-k'}$ is a C-character in B_0, satisfying $f_3(w^{-s})=f_3(g^rw^{-s})$

---

[25] Another proof of this fact: from $d(g^*)=d(g'')^{1+\vartheta''}=d(g'')^2$ one derives that d is a C-character of order m. But it follows from Theorem II.5.2 that m is exactly the order of the C-character group of the cyclic group $\{g\}$.

$=f_2(g^r w^{-s})b(g^r w^{-s})^{-k'}=f_2(g^r w^{-s})\neq 1$; and from $f_3(w)^{-s}=f_3(w^{-s})\neq 1$ we infer $f_3(w)\neq 1$, showing that again w is not mapped upon 1 by B_0.

If $b(w)\neq 1$, but w is not of order p, then $p=2$, $g^*\neq 1$ and $w^2=g^*$. Denote by g'' an element in $\{g\}$ inducing in E an automorphism of order 2. Then $g^*=g''^2$, and the integer corresponding to g'' is of the form $g''\equiv 1+2^{\mu-1}$ modulo m. Since $b(g^*)=b(g''^2)=b(g'')^{1+g''}=b(g'')^{2+2^{\mu-1}}$ is of order 2, it follows that $b(g'')$ is of order 4 whereas $b(w)$ is of order 2 or 4 and we find again an integer r such that $b(w)$ and $b(g^r)$ are of equal order, an odd integer s such that $b(w)^s=b(g^r)$; and we may now show, exactly as in the preceding paragraph, that w is not mapped upon 1 by B_0.

Thus we have shown that all the hypotheses of Lemma IV.1.3 are satisfied by the group B; and hence it follows that B is the full C-character group of G.

Case 2. $p=2$, the order of G/G_C is 2 and condition (2) *is satisfied by G.* Then the integer g corresponding to the element g in G is of the form $g\equiv -1+2^{\mu-1}$ modulo m; and $g^*=g^2$ is an element in G_C such that $g^{*2}=1$. Since $G^2\leqq G_C$, and since every element in G, not in G_C, has the form xg for x in G_C, it follows from $(xg)^2=x^{1+g}g^*=x^{2^{\mu-1}}g^*$ that G^2 is obtained by adjoining g^* to G_C^2; and it follows from (2) that g^* is not a square in G_C so that in particular $g^*\neq 1$.

There exists in every complete group B of C-characters of G a C-character b such that $b(g^*)\neq 1$. Since g^* is an element of order 2 in G_C, $b(g^*)$ is an element of order 2; and we deduce from $b(g^*)=b(g^2)=b(g)^{1+g}=b(g)^{2^{\mu-1}}$ that $b(g)$ is an element of order $2^\mu=m$ in E, that is $b(g)$ generates E; and this implies in particular that every C-character of $\{g\}$ is induced by a power of b.

If w is an element in G_C whose order modulo $\{g\}$ is 2, then $w^2=1$, since $w^2=g^*$ contradicts (2). Clearly $b(w)$ is either an element of order 2, as is $b(g^*)$, or is 1, as is $b(g^4)$; and thus there exists an integer r such that $b(g^r)$ and $b(w)$ are of equal order. Hence there exists an odd integer s such that $b(w)^s=b(g^r)$. Now we may show by the same arguments, as used in Case 1 above, that there exists a C-character in B which maps g upon 1 and w upon an element not 1; and we infer from Lemma IV.1.3 that the complete group B of C-characters of G is the full C-character group of G.

This completes the proof of the sufficiency of the conditions of our theorem.

Case 3. p is odd, but condition (1) *is not satisfied by G.* Then $1<\mu$ and the order of G/G_C is different from 1 and prime to p. It is a consequence of II.1 that the integers corresponding to elements y, not in G_C, meet the requirement $y-1$ is prime to p.

Consider the group B of all the C-characters f of G, satisfying $f(g)$ is in E^p.

Since the cross-cut of $\{g\}$ and G_C is 1, it follows from the C-completeness of G and Lemma I.3.4 that every C_0-character of G_C in E is induced by one and only one C-character in B which maps g upon 1. Hence it follows from

Theorem I.1.4 that every element y in G which is not in $\{g\}$ is mapped upon elements, not 1, by C-characters in B, since $y=xg^i$ for $x\neq 1$ in G_C. If v is an element, not 1, in E^p, then v^{1-c} is a C-character in B satisfying $v^{1-g^i}\neq 1$ for $g^i\neq 1$; and thus we have shown the completeness of the group B.

But B is not the full C-character group of G, since the C-character e^{1-c} for e a generator of E cannot be in B, as e^{1-g} is not in E^p. Thus we have shown that condition (1) is a necessary condition.

Case 4. $p=2$, *but condition* (2) *is not satisfied by* G. Then G/G_C is of order 2; the integer g corresponding to the element g in G satisfies $g\equiv -1+2^{\mu-1}$ modulo m; and the element $g^*=g^2$ whose order is 1 or 2 belongs to G_C^2; and $2<\mu$, since g is not in G_C.

Case 4.1. $g^*=1$. Consider the group B of all the C-characters of G which map g upon an element in E^4.

Then it is readily verified that there exists to every element not in $\{g\}$ a C-character in B which does not map it upon 1. If v generates E, then the C-character $v^{2(1-c)}$ is in B, since $v^{2(1-g)}=v^4$; and g is not mapped upon 1 by this C-character, since $v^4\neq 1$. But B does not contain the C-character v^{1-g}, that is, B is a complete group of C-characters which is not the full C-character group.

Case 4.2. $g^*\neq 1$. Then g^* is of order 2 and there exists an element w in G_C such that $w^2=g^*$. There exists, because of the C-completeness of G, a C-character f of G which maps g^* upon an element of order 2; and we denote by B the group of C-characters of G which is generated by f and by those C-characters of G which map g and w upon 1.

Since every C_0-character of G_C which maps w (and therefore g^*) upon 1 is induced by one and only one C-character in B which maps g upon 1, it follows that there exists to every element y in G which is not in the subgroup W generated by g and w a C-character in B which does not map y upon 1.

Since $f(g^*)$ is of order 2, and since $f(g^*)=f(g^2)=f(g)^{1+g}=f(g)^{2^{\mu-1}}$, it follows that $f(g)$ is of order m. Since the order 4 of w and $f(w)$ is smaller than m, and since every element in W, not in G_C, is of the form gw^i, it follows that $f(gw^i)=f(g)f(w)^i\neq 1$, that the elements, not in W_C, are mapped upon elements, not 1, by C-characters in B. Since W_C is generated by w, and since $f(w^2)=f(g^*)\neq 1$, we see finally that B is a complete group of C-characters of G.

From the argument used in the second paragraph of this Case 4.2 and from the fact that the order of the C-character f is m, since $f(g)$ is of order m, it follows that the order of B is exactly $2^{\mu-2}$ times the order of G_C. But it follows from Theorem II.5.2 that the order of the full C-character group of G is exactly $2^{\mu-1}$ times the order of G_C so that B is not the full C-character group of G.

This completes the proof of the necessity of condition (2); and we have completed the proof of our theorem.

IV.3. **The case of primary E and non-cyclic G/G_C.** Since a primary cyclic group whose group of automorphisms is not cyclic is of necessity of order a power of 2 [at least 8], we shall impose throughout this section the following hypotheses(26).

(IV.3.*) E is a cyclic group of order $m=2^\mu$ where $2<\mu$, C is a homomorphism of the group G into the group of automorphisms of E such that G/G_C is not cyclic, and G is C-complete.

It will be convenient to derive first some general properties of such groups and their C-characters.

LEMMA IV.3.1. (a) *There exists a basis g, z of G modulo G_C such that z induces an inversion in E and such that the integer corresponding to the element g under C is of the form $g\equiv -1+2^j g_0$ modulo m where g_0 is odd and $1<j<\mu$.*

(b) *If g, z is a basis of G modulo G_C, meeting the requirements of* (a), *if $n=2^r$ is the order of the automorphism g of E (and therefore half the order of G/G_C), if $g^*=g^n$ and G^* the group generated by g and z, then $z^2=g^{*2}=1$, $G=G_CG^*$, G_C^* is generated by g^* and the commutator $[g, z]$ whose order 2^h is a divisor of $2^{\mu-1}$.*

(c) *If y, z are elements in G such that z induces the inversion in E, and if f is a C-character of the group generated by y and z, then $f([z, y])^v=f(z)^{1-v}f(y)^{-2}$; and the C-character f^2 belongs to the principal genus of the group generated by y and z if, and only if, $f([z, y])=1$.*

It should be noted that the *commutator* of two elements v, w is defined by $[v, w]=vwv^{-1}w^{-1}$.

Proof. It is an immediate consequence of our hypotheses (IV.3.*) and of II.1.B that there exists a basis y, z of G modulo G_C such that z is an inversion of E; and it is readily verified that either the basis y, z or the basis yz, z of G modulo G_C meets the requirements of (a).

If the basis g, z of G modulo G_C meets the requirements enunciated in (a), then the automorphism g of E leaves only the elements of an order dividing 2 invariant; and it follows from the C-completeness of G and Theorem III.1.2 that $z^2=g^{*2}=1$. Since the group of automorphisms of E which are induced by elements in G is the direct product of a cyclic group of order 2 by a cyclic group of order n, and since this group is isomorphic to G^*/G_C^*, it follows that G_C^* is generated by g^* and the commutator $[g, z]$. This completes the proof of (b) with the exception of the assertion concerning the order of $[g, z]$.

Suppose now that the element z in G induces the inversion in E, that y is some element in G, that Y is the subgroup generated by y and z, and that f is some C-character of Y. Then

(26) Without restating them in the hypotheses of the various theorems of this section.

$$f(z)^{y-1}f(y)^2 = f(z)^y f(y)\,[f(y)^{-1}f(z)]^{-1} = f(zy)f(yz)^{-1}$$
$$= f(zy)f[(yz)^{-1}]^{zy} = f[(yz)^{-1}zy] = f(zy^{-1}zy);$$

and substituting y^{-1} for y we obtain:

$$f(zyzy^{-1}) = f(z)^{y^{-1}-1}f(y^{-1})^2 = f(z)^{y^{-1}-1}f(y)^{-2y^{-}}$$

or

$$f([z, y])^y = f(z)^{1-y}f(y)^{-2}.$$

Since y is odd and $1-y$ is even, it follows from this formula that $f([z, y]^{2^{\mu-1}}) = f([z, y])^{2^{\mu-1}} = 1$; and we infer from the C-completeness of G that $[z, y]^{2^{\mu-1}} = 1$, completing the proof of (b).

If $f^2(x) = v^{1-x}$ for v in E and x in Y, then we infer from the above formula and the evenness of $1-y$ that $f([z, y])^y = v^{(1-z)(1-y)2^{-1}-(1-y)} = 1$ so that $f([z, y]) = 1$; and if conversely $f([z, y]) = 1$, then it follows from the above formula that $f(y)^2 = f(z)^{1-y}$; and it follows from Theorem II.3.1(2) that f^2 belongs to the principal genus of Y.

LEMMA IV.3.2. *If g, z is a basis of G modulo G_C, and if z induces the inversion in E, then the commutator subgroup G' of G is obtained by adjoining the commutator $[g, z]$ to G_C^2.*

Proof. If x is in G_C and y in G, then the commutator $x^{1-y} = [x, y^{-1}]$ is in G_C^2, since $1-y$ is even; and in particular $x^{1-z} = x^2$. Now it is clear how to complete the proof, since subgroups of G_C are by Theorem I.3.1 and Corollary I.3.2 normal subgroups of G.

LEMMA IV.3.3. *If $G' = G_C^2$, then there exists a strictly complete group of C-characters of G which is not the full C-character group of G.*

Proof. Suppose that the elements g, z in G form a basis of G modulo G_C which meets the requirements of Lemma IV.3.1(a). It is a consequence of our hypothesis that the commutator $[g, z]$ belongs to G_C^2 and that there exists therefore an element w in G_C, satisfying $(w^{g^{-1}(1-2^{i-1}g_0)})^2 = [z, g]$, since $g^{-1}(1-2^{i-2}g_0)$ is odd. It is clear that the elements g, wz form a basis of G modulo G_C which meets the requirements of Lemma IV.3.1(a); and one finds that

$$[g, wz] = gwzg^{-1}(wz)^{-1} = w^{g^{-1}}[g, z]w^{-1} = w^{g^{-1}-1}[g, z] = 1.$$

Hence we may assume without loss of generality that the basis g, z of G modulo G_C satisfies beyond the conditions of Lemma IV.3.1(a) the additional condition $[g, z] = 1$ so that the subgroup G^* of G which is generated by g and z is *an abelian subgroup*. It is a consequence of Lemma IV.3.1(b)

that G_C^* is generated by the element $g^* = g^n$ for n the order of the automorphism g of E, and that $g^{*2} = 1$.

Case 1. $g^* = 1$. Then we consider the group B of C-characters of G which is generated by the principal genus of G and by all those C-characters of G which map G^* upon 1. Since B contains the principal genus, elements not in G_C are not mapped upon 1 by all the C-characters in B. Since 1 is the cross-cut of G^* and G_C, it follows from Lemma I.3.4 that every C_0-character of G_C in E is induced by one and only one C-character of G which maps G^* upon 1 and which therefore belongs to B; and thus it follows from the C-completeness of G and Theorem I.1.4 that 1 is the only element in G_C (and therefore in G) which is mapped upon 1 by all the C-characters in B. Thus B is shown to be strictly complete. Since B is the direct product of the principal genus and of the group of C-characters of G which map G^* upon 1, and since the order of the latter group is by Theorem I.1.3 and the C-completeness of G (and by a previous remark) exactly the order of G_C, it follows from Theorem II.2.2(a) that the order of B is $2^{\mu-1}$ times the order of G_C. On the other hand we infer from Theorem II.5.2 that the order of the full C-character group of G is exactly 2^μ times the order of G_C showing that B cannot be the full C-character group of G.

Case 2. $g^* \neq 1$. The cross-cut G_C^* of G^* and G_C is in this case by Lemma IV.3.1(b) the cyclic group of order 2 which is generated by g^*.

Denote by B^* the group of all C-characters of G which map G^* upon 1. It is an immediate consequence of the C-completeness of G, of Lemma I.3.4 and Theorem I.1.4 that every C_0-character of G_C in E which maps g^* upon 1 is induced by one and only one C-character in B^*; and it follows from Theorem I.1.3 that the order of B^* is half the order of G_C; and that the elements not in G^* are mapped upon elements not 1 by characters in B^*.

Denote by B^{**} the group of C-characters of G which is generated by adjoining the principal genus of G to B^*. The cross-cut of B^* and the principal genus of G is evidently 1. Thus the order of B^{**} is $2^{\mu-2}$ times the order of G_C, since the order of the principal genus is by Theorem II.2.2(a) exactly $2^{\mu-1}$. Clearly the elements, not in G_C^*, are mapped upon elements different from 1 by suitable C-characters in B^{**}.

Since G is C-complete, there exists a C-character f of G such that $f(g^*) \neq 1$. This C-character f does not belong to B^{**}, since the characters in B^* as well as in the principal genus map g^* upon 1. From $[g, z] = 1$ we infer $f([g, z]) = 1$; and hence it follows from Lemma IV.3.1(c) that f^2 induces in G^* a character of the principal genus of G^*. There exists therefore an element v in E such that $f^2(x) = v^{1-x}$ for x in G^* so that the C-character $b(x) = f^2(x)v^{x-1}$ belongs to B^*. Hence f^2 itself belongs to B^{**}; that is, f is of order 2 modulo B^{**}. We denote by B the group of C-characters of G which is generated by adjoining f to B^{**}. It follows from what we have shown thus far that B is a strictly complete

group of C-characters of G; and that the order of B is $2^{\mu-1}$ times the order of G_C, since the order of B is twice the order of B^{**}. But we infer again from Theorem II.5.2(a) that the order of the C-character group of G is exactly 2^{μ} times the order of G_C showing that the strictly complete group B of C-characters of G is not the full C-character group of G; and this completes the proof.

It is a consequence of Lemma IV.3.1(a) that G/G_C is the direct product of a cyclic group Z and a cyclic group Z' where the elements in Z induce in E the inversion (so that Z is of order 2) whereas Z' is generated by an element to which corresponds under C an integer of the form $-1+2^j g_0$ modulo m where g_0 is odd and $1<j<\mu$. It is readily seen that Z and Z' are uniquely determined by these properties. The normal *subgroup* $A=A(G, C)$ of G which contains G_C and satisfies $Z'=A/G_C$ is consequently uniquely determined by G and C.

LEMMA IV.3.4. *If the basis g, z of G modulo G_C meets the requirements of Lemma* IV.3.1(a), *if n is the order of the automorphism g of E and $g^*=g^n$, then A is obtained by adjoining g to G_C; and the cross-cut of A^2 and G_C is generated by g^* and G_C^2.*

Proof. It is clear that the coset $G_C g$ is a generator of the cyclic group $Z'=A/G_C$; and that therefore A is obtained by adjoining g to G_C. The elements in A whose squares are in G_C are clearly contained in the cosets G_C and $G_C g^{n^{2-1}}$ of A/G_C, as these make up the cyclic subgroup of order 2 of Z'. The cross-cut of the groups A^2 and G_C therefore certainly contains the elements in G_C^2 and the element $(g^{n^{2-1}})^2=g^*$. Any further element is of the form $(xg^{n^{2-1}})^2=x^{1+g^{-n^{2-1}}}g^*$ for x in G_C; and this element is contained in the group generated by adjoining g^* to G_C^2, since the exponent of x is certainly an even integer; and this completes the proof.

LEMMA IV.3.5. *If the order of G/G_C is not* 4 (*and therefore divisible by* 8), *if the commutator subgroup $G'\leqq A^2$, then there exists a complete group of C-characters of G which is not the full C-character group of G.*

Proof. This is an immediate consequence of Lemma IV.3.3, in case $G'=G_C^2$; and hence we may assume that $G_C^2<G'\leqq A^2$. Since $G'\leqq G_C$, and since the order of G'/G_C^2 as well as the order of[27] $(G_C\cap A^2)/G_C^2$ is at most 2 (as follows from Lemmas IV.3.2 and IV.3.4), it follows that $G_C^2<G'=G_C\cap A^2$. If g, z is some basis of G modulo G_C which meets the requirements of Lemma IV.3.1(a), then it follows from Lemmas IV.3.2 and IV.3.4 that $[g, z]\equiv g^*$ modulo G_C^2 where $g^*=g^n$ for n the order of the automorphism g of E; and that neither $[g, z]$ nor g^* is in G_C^2 (so that g^* is, by Lemma IV.3.1(b), of order 2). Since the integer $(1-g)g^{-1}$ is of the form $(1-g)g^{-1}\equiv 2(1-2^{i-1}g_0)g^{-1}$

[27] $S\cap T$ denotes the cross-cut of the sets S and T.

modulo m where the factor of 2 is odd, there exists an element w in G_C such that $g^* = w^{(1-g)g^{-1}}[g, z] = [g, wz]$. Since the elements g, wz form, exactly as g, z, a basis of G/G_C which meets the requirements of Lemma IV.3.1(a), we may assume without loss of generality that g, z is a basis of G modulo G_C which meets the requirements of Lemma IV.3.1(a) and which satisfies $[g, z] = g^*$.

We note that the order of the automorphism g of E is a multiple of 4 (or $1 < r$), since the order of G/G_C is a multiple of 8.

Since g^* is an element of order 2 in G_C which is not a square in G_C there exists a C_0-character f_1 of G_C in E which maps G_C^2, but not g^* upon 1 (cp. Theorem I.1.4!); and it is clear that $f_1^2 = 1$. Since G is C-complete, we infer from Theorem I.3.1 the existence of a C-character f of G which induces f_1 in G_C. Since n is the order of the automorphism g of E, and since g^* and $f(g^*)$ are elements of order 2, we infer from II.1.B that

$$f(g^*) = f(g^n) = f(g)^{1+g+\cdots+g^{n-1}} = f(g)^{2^{\mu-1}};$$

and this shows that $f(g)$ is an element of order 2^μ, so that $f(g)$ generates E. From Lemma IV.3.1(c) we infer that

$$f(g^*)f(g)^2 = f([z, g])^g f(g)^2 = f(z)^{1-g} = f(z)^{2-2^{j g_0}}$$

showing that $f(z)^2$ is of order $2^{\mu-1}$ and $f(z)$ of order 2^μ.

The element $g^{n2^{-1}}$ induces in E an automorphism of order 2 and the integer corresponding to $g^{n2^{-1}}$ under C is of the form $1+2^{\mu-1}$ modulo m, since $n2^{-1}$ is even. Hence we find that

$$f(g^*) = f(g^{n2^{-1}2}) = f(g^{n2^{-1}})^{1+g^{n2^{-1}}} = f(g^{n2^{-1}})^{2+2^{\mu-1}} = f(g^{n2^{-1}})^2,$$

since $f(g^*)$ is of order 2 and since $1+2^{\mu-2}$ is odd.

The C-character f^2 of G maps G_C upon 1. If w is an element in G, not in G_C, whose order modulo G_C is two, then

$$w \equiv z \quad \text{or} \quad g^{n2^{-1}} \quad \text{or} \quad g^{n2^{-1}}z \text{ modulo } G_C.$$

Accordingly we find that $f(w)^2 = f(z)^2$ or $f(g^{n2^{-1}})^2$ or $f(g^{n2^{-1}})^{-2}f(z)^2$. In the first of these cases $f(w)^2$ is of order $2^{\mu-1}$; in the second case $f(w)^2$ is of order 2; and in the third case $f(w)^2$ is of order $2^{\mu-1}$, since it is the product of an element of order 2 by an element of order $2^{\mu-1}$. In all three cases $f(w)^2 \neq 1$; and this shows that f^2 maps an element upon 1 if, and only if, this element is in G_C.

Consider now the group B_1 of all the C-characters of G which map g and z upon 1. If G^* is the subgroup, generated by g and z, then the cross-cut G_C^* of G^* and G_C is, by Lemma IV.3.1(b), the cyclic subgroup of order 2 generated by g^*. Hence it follows from the C-completeness of G and Lemma I.3.4 that every C_0-character of G_C in E which maps g^* upon 1 is induced by one

and only one C-character in B_1. Thus the order of B_1 is half the order of G_C; and there exists to every element in G_C, not in G_C^*, a C-character in B_1 which does not map it upon 1.

Denote by B the group of C-characters of G, generated by f and B_1. The order of B is 2^μ times the order of B_1, since the order of $f(z)$ is 2^μ, that is, the order of B is $2^{\mu-1}$ times the order of G_C. The group B is complete, since elements not in G_C are mapped upon elements, not 1, by f, since the elements in G_C, not in G_C^*, are mapped by C-characters in B_1 upon elements different from 1, and since $f(g^*) \neq 1$. But it follows from Theorem II.5.2 that the order of the full C-character group of G is 2^μ times the order of G_C, showing that the complete group B of C-characters of G is not the full C-character group of G.

LEMMA IV.3.6. *If G/G_C is of order 4, if $A^2 = G_C^2$, then there exists a complete group of C-characters of G which is not the full C-character group of G.*

Note that $G^2 \leqq G_C$, since G/G_C is the direct product of two cyclic groups of order 2.

Proof. It is a consequence of Corollary III.1.3 that every C-character of the subgroup A of G is induced by some C-characters of G, since G is C-complete. It is a consequence of $A^2 = G_C^2$ and of Theorem IV.2.2(a) that there exists a complete group D of C-characters of A which is not the group of all the C-characters of A. Denote by B the group of all the C-characters of G which induce in A C-characters in D. Since not every C-character of A is induced by C-characters in B, and since every C-character of A is induced by some C-character of G, it follows that B is not the full C-character group of G.

There exists a C-character f of G which maps A upon 1 and the elements, not in A, upon the element of order 2 in E, since G/A is of order 2, and since the automorphisms of E leave the element of order 2 invariant. Clearly f belongs to B; and thus it follows that B is complete, since B induces in A the complete group D.

THEOREM IV.3.7. *The C-character group of G is the only complete group of C-characters of G if, and only if,*

(i) *G' is not part of A^2 in case the order of G/G_C is a multiple of 8; and*

(ii) *neither G' nor A^2 is equal to G_C^2 in case G/G_C is of order 4.*

Proof. The necessity of condition (i) is a restatement of Lemma IV.3.5 whereas the necessity of (ii) may be derived from Lemmas IV.3.3 and IV.3.6.

In the proof of the sufficiency of the conditions (i), (ii) we distinguish two cases:

A. $G' > A^2$. We use a basis g, z of G modulo G_C which meets the requirements of Lemma IV.3.1(a), denote by n the order of the automorphism g and put $g^* = g^n$. By G^* we denote the subgroup generated by g and z and by A^* the subgroup generated by g and $[g, z]$. Then it follows from Lemma

IV.3.1 that $G_C^* = A_C^*$ is generated by g^* and $[g, z]$ where $g^{*2} = 1$ and where the order of the commutator $[g, z]$ shall be denoted by 2^h. It is a consequence of Lemmas IV.3.2 and IV.3.4 that the hypothesis A is equivalent to the two statements:

A'. $[g, z] \not\equiv g^*$ modulo G_C^2 and $[g, z] \not\equiv 1$ modulo G_C^2.

Suppose now that B be a complete group of C-characters of G. Then B induces both in A and in A^* a complete group of C-characters; and it is a consequence of condition (ii) and Theorem IV.2.2(2) that:

(*) *Every C-character of A, A^* and of the cyclic group $\{g\}$ generated by g is induced by some C-character in B.*

It is a consequence of Theorem II.5.2 that the order of the [cyclic] C-character group of[28] $\{g\}$ is 2^μ, if $g^* \neq 1$, and $2^{\mu-1}$, if $g^* = 1$. Hence there exists a C-character b_1 in B such that $b_1(g)$ is of order 2^μ, if $g^* \neq 1$, and of order $2^{\mu-1}$, if $g^* = 1$. If f is any C-character of G, then there exists an integer i such that $b_1(g)^i = f(g)$. Consequently there exists a C-character b_2 in B such that $b_2(g) = 1$ and such that the order of $b_2([g, z])$ is 2^h, if the cross-cut of the cyclic groups $\{g\}$ and $\{[g, z]\}$ is 1, and such that the order of $b_2([g, z])$ is 2^{h-1}, if $g^* \neq 1$ is a power of $[g, z]$. It is a consequence of A' that $1 < h$, if $g^* \neq 1$ is a power of $[g, z]$ so that b_2 is different from 1 on A^*. These two C-characters b_1 and b_2 are independent on A^*; and the order of the group of C-characters of A^* induced by b_1, b_2 and their products is exactly $2^{\mu-1}$ times the order of A_C^* so that every C-character of A^* is induced by a combination of b_1 and b_2.

It is a consequence of Lemma IV.3.1(c) that

$$b_2([z, g]) = b_2(z)^{(1-g)g^{-1}} = b_2(z)^{2(1-2^{j-1}g_0)g^{-1}}$$

and that therefore the order of $b_2(z)$ is twice the order of $b_2([z, g])$. The order of the C-character of G^*, induced by b_2, is therefore twice the order of the C-character of A^*, induced by b_2, since the latter is the same as the order of $b_2([z, g])$. The group of C-characters of G^*, induced by the combinations of b_1 and b_2, has therefore the order 2^μ times the order of G_C^* (note that $G_C^* = A_C^*$); and thus it follows from Theorem II.5.2 that

(**) *every C-character of G^* is induced by some combination of the C-characters b_1 and b_2 in B.*

Suppose now that W_0 is a coset of order 2 in G_C/G_C^* and that W is the subgroup of G, generated by adjoining W_0 to A^*. It is a consequence of hypothesis A' that W_0 contains an element w satisfying $w^2 = 1$ or $w^2 = g^*$ (the latter can happen only if the order n of the automorphism g of E is not 2). Since $b_2(g^*) = 1$, it follows that $b_2(w)$ is an element of order 1 or 2 showing that b_2 induces C-characters of equal order in W and in A^*. The order of

---

[28] It should be remembered that $\{g\}$ denotes the cyclic group, generated by the element g.

$b_1(w)$ is a divisor of 4 and 4 is a divisor of $2^{\mu-1}$ and therefore of the order of b_1, showing that b_1 induces C-characters of equal order in W and in A^*. Thus it follows that the group D of C-characters, generated by b_1 and b_2, induces in W a group of C-characters whose order is $2^{\mu-1}$ times the order of A_C^*. Since w is not in A_C^*, and is of order 2 modulo A_C^*, it follows from Theorem II.5.2 that the C-character group of W is of order 2^μ times the order of A_C^*; and hence there exists a C-character r of W which is not induced by C-characters in D. But $W \leqq A$; and hence it follows from (ii) and Theorem IV.2.2(2) that every C-character of W is induced by some C-character in B. In particular there exists a C-character b in B which induces r in W. We infer from (**) the existence of integers i', i'' such that b and $b_1^{i'}b_2^{i''}$ coincide on G^*; and we put $b_3 = bb_1^{-i'}b_2^{-i''}$. This C-character b_3 certainly belongs to the group B^* of all the C-characters in B which map G^* upon 1. Since b_3 cannot map every element in W upon 1, and since b_3 maps every element in A^* upon 1 (as A^* is part of G^*), it follows that $b_3(w) \neq 1$; and this implies $b_3(W_0) \neq 1$. Hence there exists to every element in G_C whose order modulo G^* (or $G_C^* = A_C^*$) is 2 a C-character in B^* which does not map it upon 1. Now we infer from (**) and Lemma IV.1.3 that B is the full C-character group of G, as was to be shown.

B. $G' \leqq A^2$. In this case we infer from (i) that the order of G/G_C is 4. Using condition (ii) we infer now—exactly as in the beginning of the proof of Lemma IV.3.5—the existence of a basis g, z of G modulo G_C meeting the requirements of Lemma IV.3.1(a) and satisfying:

B'. $g^2 = g^* = [g, z]$ is an element of order 2, not in G_C^2. We note that the integer corresponding under C to the element g in G is of the form $g \equiv -1 + 2^{\mu-1}$ modulo m; and we verify that

$$[g^{-1}, z] = g^{-1}zgz = g^*gzg^{-1}g^*z = g^*[g, z]g^* = [g, z].$$

Suppse now that B is a complete group of C-characters of G. Then there exists in B a C-character such that $b(g^*) \neq 1$. Hence $b(g^*) = b(g^2) = b(g)^{1+g} = b(g)^{2^{\mu-1}}$ is an element of order 2; and $b(g)$ is an element of order 2^μ. From Lemma IV.3.1(c) we derive $b(g^*)b(g)^2 = b(g^*)^g b(g)^2 = b(z)^{1-g} = b(z)^{2+2^{\mu-1}}$. Since $b(g)^2$ is of order $2^{\mu-1}$ and $b(g^*)$ of order 2, we deduce from this last equation that $b(z)$ is of order 2^μ so that $b(z)^{2^{\mu-1}}$ is the only element of order 2 in E, namely $b(g^*)$; and hence it follows that $b(g)^2 = b(z)^2$.

If $b(g) = b(z)$, then $b(gz) = b(g)^{-1}b(z) = 1$. If $b(g) \neq b(z)$, then it follows from $b(g)^2 = b(z)^2$ that $b(z) = b(g)b(g^*) = b(gg^*) = b(g^{-1})$ since $b(g^*)$ is the element of order 2 in E; and this shows that $b(g^{-1}z) = b(g^{-1})^{-1}b(z) = 1$. In both cases there exists therefore in the group G^*, generated by g and z, an element which is not contained in G_C and which is mapped upon 1 by the C-character b. Since B induces a complete group of C-characters in G^*, there exists a C-character b' in B which does not coincide with any power of b on G^*. Denote by D the

subgroup of B, generated by b and b'. Since b is of order 2^μ on G^*, it follows that D induces in G^* a group of C-characters whose order is at least $2^{\mu+1}$. But this is by Theorem II.5.2 exactly the order of the C-character group of G^*, since G_C^* is by Lemma IV.3.1(2) and condition B′ the cyclic group of order 2, generated by g^*. Thus we have shown:

(+) *Every C-character of G^* is induced by some C-character in $D \leqq B$.*

Since $b(g)$ is an element of order 2^μ, there exists an integer i such that $b(g)^i = b'(g)$. Put $b_0 = b'b^{-i}$. Then b, b_0 generate D and b_0 is different from 1 on G^*, though $b_0(g) = 1$. Since this implies $b_0([g, z]) = b_0(g^*) = b_0(g^2) = 1$, it follows from Lemma IV.3.1(c) that $b_0(z)$ is an element of order 2.

We denote again by B^* the group of all those C-characters in B which map G^* upon 1.

If W_0 is a coset of G_C/G_C^* whose order is 2, then it follows from (ii) and condition B′ that W_0 contains an element w of order 2 which is not in G_C^*, that is $w \neq g^*$. The complete group B of C-characters of G induces in G_C a complete group of C_0-characters; and it follows from Theorem I.1.4 that every C_0-character of G_C in E is induced by some C-character in B. Hence it follows from Lemma I.1.1(b) that B contains a C-character which maps w, but not g^*, upon 1; and we may assume without loss of generality that the C-character b, considered before, has this property.

If $b_0(w) = 1$, then let f be any C-character in B such that $f(w) \neq 1$ (the existence of f is a consequence of $w \neq 1$ and of the completeness of B). There exist integers i, i_0 such that f and $b^i b_0^{i_0}$ coincide on G^*, as follows from (+); and hence $f^* = fb^{-i}b_0^{-i_0}$ is in B^*. But $f^*(w) = f(w) \neq 1$ so that B^* contains a C-character which does not map W_0 upon 1.

Suppose next that $b_0(w) \neq 1$. Then $b_0(w)$ is of order 2, that is $b_0(w) = b_0(z)$. It has been shown before that either $b(gz)$ or $b(g^{-1}z)$ is equal to 1. Hence determine $e = \pm 1$ in such a fashion that $b(g^e z) = 1$. Then $b(wg^e z) = 1$ and $b_0(wg^e z) = b_0(w)b_0(g^e z) = b_0(w)b_0(z) = 1$, since $b_0(g) = 1$, and since $b_0(w) = b_0(z)$ is of order 2. From the completeness of B we infer the existence of a C-character t in B such that $t(wg^e z) \neq 1$; and from (+) we deduce the existence of integers k, k_0 such that $t^* = tb^{-k}b_0^{-k_0}$ is in B^* (maps G^* upon 1). Hence $t^*(W_0) = t^*(w) = t^*(w)^{g^e z}t^*(g^e z)$, since $t^*(w)$ is of order 2 and $t^*(g^e z)$ is equal to 1; and therefore we find that $t^*(W_0) = t^*(wg^e z) = t(wg^e z) \neq 1$, since $b(wg^e z) = b_0(wg^e z) = 1$; and we have shown again the existence of a C-character in B^* which does not map W_0 upon 1.

But now it is an immediate inference from (+) and Lemma IV.1.3 that B is the full C-character group of G; and this completes the proof of the theorem.

THEOREM IV.3.8. *The C-character group of G is the only strictly complete group of C-characters of G if, and only if, $G_C^2 < G'$.*

Proof. It is a consequence of Lemma IV.3.2 that $G_C^2 \leqq G'$. Hence we may deduce the necessity of our condition from Lemma IV.3.3.

Assume now that $G_C^2 < G'$. We distinguish two cases:

Case 1. *The order of* G/G_C *is* 4. If $A^2 \neq G_C^2$, then our contention is a consequence of Theorem IV.3.7. Thus we assume now that $A^2 = G_C^2$. Consider a basis g, z of G modulo G_C meeting the requirements of Lemma IV.3.1(a). Then $g^* = g^2$ is in G_C^2.

If B is a strictly complete group of C-characters of G, then B induces in A a strictly complete group of C-characters; and it follows from Theorem IV.2.1 that B induces in A every C-character of A. It is a consequence of the C-completeness of G and A and of Lemma I.3.4 that there exists a C-character of A which maps g and G_C^2 upon 1 but which maps $[g, z]$ upon an element of order 2, since g^* is in G_C^2 whereas $[g, z]$ does not belong to G_C^2; and hence there exists in B a C-character b which maps both g and G_C^2 upon 1 though $b([g, z])$ is of order 2. Hence it follows from Lemma IV.3.1(c) that $b(z)^{1-g} = b([z, g])^g$; and this implies $b(z)^2 = b([z, g])$, since $b([z, g])$ is an element of order 2. The C-character b^2 of G has therefore the properties $b^2(A) = 1$, $b^2(z)$ is of order 2. Hence it follows that every C-character of A is induced by at least two C-characters in B. The order of the C-character group of A is by Theorem II.5.2 exactly $2^{\mu-1}$ times the order of G_C; and the order of the C-character group of G is exactly 2^μ times the order of G_C; and from these facts one deduces that B is the full C-character group of G.

Case 2. *The order of* G/G_C *is divisible by* 8. If G' is not part of A^2, then our contention is a consequence of Theorem IV.3.7. Thus we assume now that $G_C^2 < G' \leqq A^2$; and we prove—exactly as in the beginning of the proof of Lemma IV.3.5—the existence of a basis g, z of G modulo G_C which meets the requirements of Lemma IV.3.1(a) and which satisfies $g^n = g^* = [g, z]$ is an element of order 2 (n denotes, as always, the order of the automorphism g of E).

If B is a strictly complete group of C-characters of G, then B induces in A a strictly complete group of C-characters; and it follows from Theorem IV.2.1 that every C-character of A is induced by some C-character in B.

There exists a C_0-character of G_C in E which maps G_C^2 upon 1 and g^* upon an element of order 2, since $g^* = [g, z]$ is not in G_C^2; and it follows from the C-completeness of G and A and from Theorem I.3.1 that this C_0-character of G_C is induced by some C-character of A. Hence there exists a C-character b in B such that $b(G_C^2) = 1$ and $b(g^*)$ is the element of order 2 in E. From $b(g^*) = b(g^n) = b(g)^{1+g+\cdots+g^{n-1}}$ and from II.1.B we infer $b(g^*) = b(g)^{2^{\mu-1}}$ is an element of order 2 so that $b(g)$ is an element of order 2^μ. Clearly $b^2(G_C) = 1$. But from $b([g, z]) \neq 1$ and Lemma IV.3.1(c) we infer that b^2 does not belong to the principal genus.

From our choice of g it follows that the integer corresponding to g under C is of the form $g \equiv -1 + 2^j g_0$ modulo m for g_0 an odd integer and $1 < j < \mu$.

The integer $1-g$ is therefore divisible by 2, but not by 4; and hence there exists an element v in E such that $b(g)^2=v^{1-g}$. The C-character v^{1-x} of G belongs to B; and B contains therefore the C-character $d(x)=b(x)^2v^{x-1}$. This C-character d is not 1, since b^2 has been shown not to be in the principal genus; but d maps both g and G_C upon 1; that is, the C-character $d\neq 1$ in B maps A upon 1. Now it follows that every C-character of A is induced by at least two C-characters in B. We deduce from Theorem II.5.2 that the order of the C-character group of G is exactly twice the order of the C-character group of A, showing that B is the full C-character group of G; and this completes the proof.

IV.4. **Completeness and p-completeness of groups of C-characters.** We have treated the problem of complete groups of C-characters completely for the special case of primary E. The reduction of the general case where E is of composite order to this special case will now be accomplished by means of the following considerations.

The group B of C-characters of the group G is the direct product of its subgroups B_p which consist of all the elements of order a power of (the prime number) p, since B is abelian. A C-character of G is of order a power of p if, and only if, it maps G into $E(p)$ (using the notations (II.3.*)!); and thus B_p consists exactly of all the Cp-characters in B. It is a consequence of the definition of the subgroup $H(p)$ that $B_p(H(p))=1$; and this leads to the following definition:

The group B of C-characters of G is p-complete, if $B_p(x)=1$ implies that x is in $H(p)$.

If the group B of C-characters of G is p-complete for every p, and if x is an element in G which is mapped upon 1 by B, then $B_p(x)=1$ for every p; and consequently x belongs to the cross-cut H of all the $H(p)$. If G is C-complete, and if B is p-complete for every p, then we deduce the completeness of B. The converse of this result need not be true; and it will be the main object of this section to find criteria for the validity of the converse.

THEOREM IV.4.1. *If G is C-complete, and if p is a prime, then the following condition is necessary and sufficient for the p-completeness of every strictly complate group of C-characters of G:*

(p) *$H(p)G_C$ contains every element*[29] *in G_{Cp} whose order modulo $H(p)$ is exactly p.*

Proof. Assume first that condition (p) is not satisfied. Then there exists an element w in G_{Cp} which is not contained in $H(p)G_C$, though its order modulo $H(p)$ is p. We denote by B the group of C-characters of G which is

(29) See Lemma III.2.2 and Corollary III.3.2 for properties of the subgroup $H(p)G_C=H^*(p)$.

generated by all the Cq-characters for $q \neq p$, and by all those Cp-characters which map w upon 1. This group B contains the principal genus, since w is in G_{Cp}. Thus $B(x)=1$ implies that x is in G_C. If $x \neq 1$ is an element of order a power of q for q a prime different from p, and if x is in G_C, then it follows from the C-completeness of G and from Theorem III.3.1 that x does not belong to $H(q)$. It is a consequence of the definition of $H(q)$ that $G/H(q)$ is Cq-complete; and hence there exists a Cq-character of G which does not map x upon 1. But all the Cq-characters are in B, that is $B(x) \neq 1$. If $x \neq 1$ is an element of order a power of p in G_C, then it follows again from the C-completeness of G and from Theorem III.3.1 that x is not in $H(p)$; and it follows from the fact that w is of order p modulo $H(p)$, but does not belong to $H(p)G_C$, that $H(p)w$ and $H(p)x$ are independent elements of $G_{Cp}/H(p)$. Hence we deduce from Lemma I.1.1(b) the existence of a C_0-character d of $G_{Cp}/H(p)$ in $E(p)$ which maps $H(p)w$ upon 1, but which does not map $H(p)x$ upon 1. It follows from the Cp-completeness of $G/H(p)$ and from Theorem I.3.1 that d is induced by a Cp-character of $G/H(p)$; and d is therefore induced by a Cp-character of G. This Cp-character of G belongs to B, since it maps w upon 1; and thus we have shown that $B(x) \neq 1$. From the facts derived thus far it follows that B is a strictly complete group of C-characters of G. But it follows from the definition of B that $B_p(w)=1$, in spite of the fact that w is not in $H(p)$, that is the strictly complete group B is not p-complete, showing the necessity of the condition (p).

Assume conversely that (p) is satisfied, and that B is a strictly complete group of C-characters of G. We denote by V the subgroup of all the elements in G which are mapped upon 1 by every Cp-character in B. Then $H(p) \leqq V \leqq G_{Cp}$, since the principal genus is in B. Suppose now that w is an element in G_{Cp} whose order modulo $H(p)$ is p. Then it follows from condition (p) that w is in $H(p)G_C$. It is a consequence of Theorem III.2.1(a) that $H(p)$ contains all the elements in G_C whose orders are prime to p; and hence we may represent w in the form $w=xy$ for x in $H(p)$ and y an element of order a power of p in G_C; and it follows from the C-completeness of G that y is an element of order p, since the order of xy modulo $H(p)$ is just p, and since $w \equiv y$ modulo $H(p)$. The group B is complete and contains therefore a C-character b such that $b(y) \neq 1$. Since b induces a C_0-character in G_C, and since y is an element of order p in G_C, it follows that $b(y)$ is of order p. The group B contains the C-character $b_1=b^{mp^{-m(p)}}$ which maps every element in G upon an element in $E(p)$; that is b_1 is a Cp-character and belongs to B_p. But $b_1(w)=b_1(y)$ is of order p and therefore different from 1, since the exponent $mp^{-m(p)}$ is prime to p. Thus $B_p(w) \neq 1$ and w does not belong to V. The subgroup $V/H(p)$ of $G_{Cp}/H(p)$ consequently does not contain elements of order p; and this implies $V=H(p)$, since $G_{Cp}/H(p)$ is of order a power of p. Hence B is p-complete, as was to be shown.

EXAMPLE. Every prime number p is a divisor of $q-1$ for q a suitable prime([30]); and we denote by E the cyclic group of order p^2q. There exists an automorphism g of the group E which induces both in $E(p)$ and in $E(q)$ an automorphism of order p. If G is the cyclic group of order p, generated by g, and if C is the isomorphism which maps the element g in G upon the automorphism g of E, then $G_C=G_{Cp}=G_{Cq}=1$ so that G is C-complete and so that condition (p) is satisfied. Denote by B the group of all the Cq-characters of G. Clearly B is a complete group of C-characters, since B is a complete group of Cq-characters. But $B_p=1$, showing that B is not p-complete.

This shows that the hypothesis of strict completeness occurring in Theorem IV.4.1 cannot be omitted.

REMARK. If the principal genus of G contains every C-character of G which maps G_C upon 1, then we infer $H(p)G_C=G_{Cp}$ from Theorem II.3.2 and this condition certainly implies condition (p) of Theorem IV.4.1.

COROLLARY IV.4.2. *The C-character group of G is the only strictly complete group of C-characters of G if, and only if, condition* (p) *of Theorem* IV.4.1 *is satisfied for every prime p, and $H(2)G_{C2}^2<H(2)G'$, in case C is singular.*

Proof. Suppose first that the C-character group of G is the only strictly complete group of C-characters of G. This implies the p-completeness of every strictly complete group of C-characters of G, proving the necessity of (p). It implies furthermore that the $C2$-character group of $G/H(2)$ is the only strictly complete group of $C2$-characters of G. If C is singular, then we infer from Theorem IV.2.1 that G/G_{C2} is not cyclic; and hence it follows from Theorem IV.3.8 that $H(2)G_{C2}^2<H(2)G'$.

Suppose conversely that the conditions are satisfied, and that B is a strictly complete group of C-characters of G. Then we infer from Theorem IV.4.1 that $H(p)$ is the set of all the elements in G, mapped upon 1 by the group B_p of the Cp-characters in B. If p is odd, or if $C2$ is not singular, then we infer from Theorem IV.2.1 that B_p contains every Cp-character of $G/H(p)$ and consequently of G. If $C2$ is singular, then G/G_{C2} is not cyclic, since otherwise $H(2)G_{C2}^2=H(2)G'$. Thus we may infer from our hypothesis and from Theorem IV.3.8 that B_2 contains every $C2$-character of $G/H(2)$ and of G, showing that B is the full C-character group of G.

In the following investigations we shall make use of the subgroups $\overline{H}(p)$. Each such group is defined as the cross-cut of all the subgroups $H(q)$ for $q\neq p$; and this is equivalent to saying $\overline{H}(p)$ is the set of all the elements x in G which are mapped upon elements in $E(p)$ by every C-character of G. If G is C-complete, then the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1; and it follows from the fact that every C-character induces a C_0-character in the abelian group G_C that the cross-cut of G_C and $H(p)$ consists of all the elements in G_C whose

([30]) As follows from Dirichlet's theorem.

order is prime to p whereas the cross-cut of G_C and $\overline{H}(p)$ consists just of the elements of order a power of p in G_C.

THEOREM IV.4.3. *If G is C-complete, if p is a prime such that G/G_{Cp} is cyclic*([31]), *then the following conditions are necessary and sufficient for p-completeness of every complete group of C-characters of G:*

(p*) *$H(p)\overline{H}(p)$ contains every element in G whose order modulo $H(p)$ is exactly p.*

(p**) *If the order of G/G_{Cp} is prime to p, and if x is an element of order a prime, not p, in $G/H(p)$, then the centralizer*([32]) *of x in $G/H(p)$ contains an element different from 1 in $(H(p)\overline{H}(p))/H(p)$.*

REMARK. The condition (p) of Theorem IV.4.1 implies that elements of order p in $G_{Cp}/H(p)$ are in $(H(p)\overline{H}(p))/H(p)$, since $G_C \leqq H(p)\overline{H}(p)$; and this condition (p) is a consequence of the condition (p*) above, since $\overline{H}(p)$ is part of the cross-cut of all the G_{Cq} for $q \neq p$, and since G_C is exactly the cross-cut of all the G_{Cr}.

Proof. We precede our arguments by the proofs of some lemmas.

(1) *If the element x in $G/H(p)$ is of order a prime, not p, then the centralizer of x in $G/H(p)$ is a cyclic group T such that $G/H(p) = T(G_{Cp}/H(p))$ and such that the cross-cut of T and $G_{Cp}/H(p)$ is* 1.

We note first that $G/H(p)$ is Cp-complete. Hence $G_{Cp}/H(p)$ is, by Theorem III.1.2, a p-group which certainly does not contain the element x. It is a consequence of II.1.A that the automorphism of $E(p)$ induced by x has no fixed elements except 1; and hence it follows from Theorem III.1.2 and the Cp-completeness of $G/H(p)$ that x does not commute with any element in $G_{Cp}/H(p)$ except 1; that is, the cross-cut of T and $G_{Cp}/H(p)$ is 1.

Since G/G_{Cp} is cyclic, there exists an element g in $G/H(p)$, generating $G/H(p)$ modulo $G_{Cp}/H(p)$. The order of G/G_{Cp} is divisible by the order r of x so that the order of the automorphism g of $E(p)$ is divisible by the prime $r \neq p$; and it follows from II.1.A that the integer $g-1$ is prime to p. A certain power g^n of g induces in $E(p)$ the same automorphism as x; and we may assume without loss of generality that g has been chosen in such a fashion that n is a divisor of the order of the automorphism g of $E(p)$, that is, that nr is the order of the automorphism g of $E(p)$. Then $x' = xg^{-n}$ is an element in $G_{Cp}/H(p)$. Since g^{1-n}, $g-1$ and $g^n-1 \equiv x-1$ modulo $p^{m(p)}$ are all integers prime to p, it follows that $1+g^{-1}+\cdots+g^{1-n} \equiv g^{1-n}(1+g+\cdots+g^{n-1}) \equiv g^{1-n}(g^n-1)/(g-1)$ modulo $p^{m(p)}$ is an integer prime to p; and hence there exists an element s in $G_{Cp}/H(p)$ such that $s^{1+g^{-1}+\cdots+g^{1-n}} = x'$. But then we deduce from Theorem III.1.2 and the Cp-completeness of $G/H(p)$ that

([31]) This hypothesis is automatically satisfied if p is odd. The case excluded by this hypothesis is treated in Theorem IV.4.4 below.

([32]) The centralizer of the element x in the group K consists of all the elements z in K such that $zx = xz$.

$$(sg)^n = s^{1+g^{-1}+\cdots+g^{1-n}}g^n = x'g^n = xg^{-n}g^n = x.$$

Clearly $sg=t$ belongs to T; and from $g\equiv t$ modulo $G_{Cp}/H(p)$ we infer that $G/H(p)=T(G_{Cp}/H(p))$. The cyclicity of T is a consequence of the facts that the cross-cut of T and $G_{Cp}/H(p)$ is 1, and that G/G_{Cp} is cyclic. This completes the proof of (1).

(2) *If x is an element of order p in $G/H(p)$, but not in $G_{Cp}/H(p)$, then every C_0-character of $G_{Cp}/H(p)$ is induced by some Cp-character of $G/H(p)$ which maps x upon* 1.

The order of G/G_{Cp} is of the form pn; and because of the cyclicity of G/G_{Cp} there exists an element g in $G/H(p)$ such that g^n and x induce the same automorphism in $E(p)$ and such that g generates $G/H(p)$ modulo $G_{Cp}/H(p)$. Clearly $x'=xg^{-n}$ is an element in $G_{Cp}/H(p)$. Then we infer from the Cp-completeness of $G/H(p)$ and Corollary I.3.2 that

$$1 = x^p = (x'g^n)^p = x'^{1+g^{-n}+\cdots+g^{-n(p-1)}}g^{np}$$

or $g^*=g^{np}=x'^{-(1+g^{-n}+\cdots+g^{-n(p-1)})}$. We note that g^* generates the cross-cut $\{g\}_{Cp}$ of $G_{Cp}/H(p)$ and of the cyclic group $\{g\}$, generated by g. Since $G/H(p)$ is Cp-complete, so is its subgroup $\{g\}$; and it follows from Theorem I.3.1 that every C_0-character of $\{g\}_{Cp}$ is induced by some Cp-character of $\{g\}$. Furthermore we have

$$\begin{aligned} 1 + g^{-n} + \cdots + g^{-n(p-1)} &\equiv g^{-n(p-1)}(1 + g^n + \cdots + g^{n(p-1)}) \\ &\equiv g^n(1 + g^n + \cdots + g^{n(p-1)}) \text{ modulo } p^{m(p)}, \end{aligned}$$

since $g^{np}\equiv 1$ modulo $p^{m(p)}$.

Since the C-character group of a cyclic group is by Lemma III.1.1 itself a cyclic group, and since $\{g\}$ is Cp-complete, there exists a Cp-character d of $\{g\}$ with the property $d(g^i)=1$ implies $g^i=1$. Since x' is in $G_{Cp}/H(p)$, and since Cp-characters are C_0-characters in $G_{Cp}/H(p)$, we find

$$d(x'^{-g^n(1+g^n+\cdots+g^{n(p-1)})}) = d(g^*) = d(g^{np}) = d(g^n)^{1+g^n+\cdots+g^{n(p-1)}}.$$

Remembering that np is the order of the automorphism g of $E(p)$ one readily deduces from the last identity that the order of x' is a factor of the order of $d(g^n)$.

If now f is any C_0-character of $G_{Cp}/H(p)$ in $E(p)$, then there exists an integer t such that $d(g^n)^t=f(x'^{-g^n})$, since the order of $f(x'^{-g^n})$ is a divisor of the order of x'; and we verify that

$$\begin{aligned} d(g^*)^t &= d(g^{np})^t = d(g^n)^{t(1+g^n+\cdots+g^{n(p-1)})} \\ &= f(x'^{-g^n})^{1+g^n+\cdots+g^{n(p-1)}} = f(x'^{-g^n(1+g^n+\cdots+g^{n(p-1)})}) \\ &= f(g^*). \end{aligned}$$

Hence we infer from Lemma I.3.4 the existence of a Cp-character f_1 of $G/H(p)$ which induces d^t in $\{g\}$ and f in $G_{Cp}/H(p)$; and this character f_1 satisfies $f_1(x)=f_1(x'g^n)=f_1(x')^{g^n}f_1(g^n)=f(x'^{g^n})d(g^n)^t=f(x'^{g^n})f(x'^{-g^n})=1$, as was to be shown.

Suppose now that every complete group of C-characters of G is p-complete. Then we denote by B_p' the group of C-characters which is generated by all the Cq-characters for $q\neq p$.

Assume first that the element x in $G/H(p)$ is of order p. If x were in $G_{Cp}/H(p)$, then we inferred from Theorem IV.4.1(p) that x is in $G_CH(p)/H(p)\leqq(\overline{H}(p)H(p))/H(p)$. Thus we consider the case where x is not in $G_{Cp}/H(p)$. Then we denote by B_p the group of all the Cp-characters of G (or $G/H(p)$) which map x upon 1; and we put $B=B_p'B_p$. This group is certainly not p-complete, as B_p maps upon 1 all the elements in the subgroup $\{x\}$ of order p of $G/H(p)$. If y is an element in $G/H(p)$, but not in the subgroup generated by x and $G_{Cp}/H(p)$, then there exists(33) a Cp-character in the principal genus of $G/H(p)$ which maps x, but not y, upon 1; and if y belongs to the subgroup generated by x and $G_{Cp}/H(p)$, though y does not belong to $\{x\}$, then we infer from (2) the existence of a Cp-character in B_p which does not map y upon 1. This shows that $\{x\}$ is the subgroup of those elements in $G/H(p)$ which are mapped upon 1 by every Cp-character in B_p. It is a consequence of the definition of B_p' and $\overline{H}(p)$ that $\overline{H}(p)$ is the set of all the elements in G mapped upon 1 by all the C-characters in B_p'; and hence it follows that the set of elements mapped upon 1 by all the C-characters in B is just the cross-cut X^* of $\overline{H}(p)$ and the subgroup X of G which contains $H(p)$ and satisfies $\{x\}=X/H(p)$. Since B is not p-complete, it follows from our present hypothesis that $X^*\neq 1$. Since G is C-complete, it follows that the cross-cut of $H(p)$ and $\overline{H}(p)$ is 1; and since $X/H(p)$ is of order p, we deduce that $X\leqq H(p)\overline{H}(p)$, showing the necessity of condition (p*).

To show the necessity of condition (p**) we consider an element x in $G/H(p)$ whose order is a prime $r\neq p$. Then we infer from (1) the existence of an element g in $G/H(p)$ such that g generates $G/H(p)$ modulo $G_{Cp}/H(p)$ and such that $g^n=x$ where nr is the order of the automorphism g of $E(p)$. We consider the group B_p of all the Cp-characters of G or $G/H(p)$ which map g upon 1. It is a consequence of (1) and of Lemma I.3.4 that every C_0-character of $G_{Cp}/H(p)$ in $E(p)$ is induced by one and only one Cp-character in B_p; and this shows that the group $\{g\}$ generated by g is the subgroup of all the elements in $G/H(p)$ which are mapped upon 1 by every Cp-character in B_p. Denote by B the product(34) of B_p' and B_p. Then the group of elements mapped upon 1 by all the C-characters in B is the cross-cut X^* of $\overline{H}(p)$ and

(33) Take an element v of order p in $E(p)$. Then $v^{1-x}=1$, though $v^{1-y}\neq 1$, since the order of y modulo G_{Cp} is neither 1 nor p, as G/G_{Cp} is cyclic.

(34) Where B_p' denotes, as before, the group generated by all the Cq-characters for q any prime not p, that is B_p' consists of all the C-characters of order prime to p.

of the subgroup X of G which contains $H(p)$ and satisfies $X/H(p)=\{g\}$. Since B is not p-complete, it is not complete, showing that $X^*\neq 1$; and noting that $\{g\}$ is exactly the centralizer of x in $G/H(p)$ (cp. (1)!), we deduce the necessity of conditon (p**).

Assume now that conditions (p*) and (p**) are both satisfied by G, C, and p, and that $B=B_p' B_p$ is a complete group of C-characters of G where B_p consists of Cp-characters of G only, whereas B_p' is generated by Cq-characters of G with $q\neq p$. This implies in particular that $B_p'(\overline{H}(p))=1$; and we deduce from the completeness of B that there exists to every element, not 1, in $\overline{H}(p)$ a Cp-character in B_p which does not map it upon 1.

Consider an element x in G whose order modulo $H(p)$ is p. Then we infer from condition (p*) that x is in $H(p)\overline{H}(p)$; and one deduces from the remark made at the end of the last paragraph the existence of a Cp-character in B_p which does not map x upon 1.

Next we consider([35]) an element x whose order modulo $H(p)$ is a prime $r\neq p$. Then we infer from (1) that the centralizer T of $H(p)x$ in $G/H(p)$ is a cyclic group, generated by an element g, such that the cross-cut of T and $G_{Cp}/H(p)$ is 1, and such that $G/H(p)=T(G_{Cp}/H(p))$. If p is a divisor of the order of G/G_{Cp}, then p is a divisor of the order of T; and it follows from (p*) that the cross-cut of T and $(\overline{H}(p)H(p))/H(p)$ is different from 1. If p is not a divisor of the order of G/G_{Cp}, then we infer from condition (p**) that the cross-cut of T and $(\overline{H}(p)H(p))/H(p)$ is different from 1. Denote by T^* the cross-cut of T and $(\overline{H}(p)H(p))/H(p)$. Then we have seen that T^* is a cyclic group different from 1; and there exists an element t in $\overline{H}(p)$ such that $H(p)t$ generates T^*. We note that $t\neq 1$. Since t is in $\overline{H}(p)$, it follows that $B_p'(t)=1$; and we infer from the completeness of B the existence of a Cp-character b in B_p such that $b(t)\neq 1$. It is a consequence of Theorem II.2.1 that every Cp-character of T belongs to the principal genus; and hence there exists an element v in $E(p)$ such that $b(y)=v^{1-y}$ for y in T. From $1\neq b(t)=v^{1-t}$ we infer $v\neq 1$; and since $x-1$ is by II.1.A prime to p, it follows that $b(x)=v^{1-x}\neq 1$. Thus we have shown that no element of order a prime in $G/H(p)$ is mapped upon 1 by every Cp-character in B (or B_p); and from this fact one deduces the p-completeness of B.

In Theorem IV.4.3 we discussed only those primes p for which G/G_{Cp} is cyclic; and this is always the case if p is odd. Thus we have to discuss the situation in case G/G_{C2} is not cyclic. Then there exists a coset Z_0 of G/G_{C2} all of whose elements induce in $E(2)$ the inversion. Apart from Z_0 there are two further cosets of order 2 in G/G_{C2}; and it follows from II.1.B that the integers corresponding under $C2$ to these two cosets are of the form $\pm 1+2^{m(2)-1}$ modulo $2^{m(2)}$. We denote by K_0 the uniquely determined coset of order 2 of G/G_{C2} to whose elements there corresponds under $C2$ the in-

([35]) Since $G/H(2)$ is a 2-group, the existence of such an element x implies that p is odd.

teger $1+2^{m(2)-1}$ modulo $2^{m(2)}$; and we denote by $K=K(G, C)$ the subgroup of G whose elements are either in G_{C2} or in K_0. In case the order of G/G_{C2} is divisible by 8 it is possible to characterize K as the subgroup between G_{C2} and G^2G_{C2} with the property that K/G_{C2} is of order 2.

THEOREM IV.4.4. *If G is C-complete, and if G/G_{C2} is not cyclic, then the following conditions are necessary and sufficient for 2-completeness of every complete group of C-characters of G:*

(i) *$H(2)\overline{H}(2)$ contains every element in the subgroup K whose order modulo $H(2)$ is 2*([36]).

(ii) *If G/G_{C2} is of order 4, then $\overline{H}(2)H(2)$ contains the following elements:*

(ii′) *Every element x in G whose order modulo $H(2)$ is 2 and which does not induce the inversion in $E(2)$, and*

(ii″) *Every element z in G which induces the inversion in $E(2)$ and which satisfies $(zy)^2\equiv y^{2^{m(2)-1}}$ modulo $H(2)$ for every y in K, y not in G_{C2}.*

Proof. We start by proving some lemmas.

(1) *If S is a subgroup of $K/H(2)$, then every C2-character of S is induced by some C2-character of G.*

It is obvious that the group of all the $C2$-characters of G induces in S a complete group of $C2$-characters. But the only complete group of $C2$-characters of $S\leqq K/H(2)$ is the group of all the $C2$-characters of S, as follows from Theorem IV.2.2, if S is not part of $G_{C2}/H(2)$, and from Theorem I.1.4, if $S\leqq G_{C2}/H(2)$.

(2) *If S is a subgroup of $K/H(2)$, and if $P(S)$ is the group of C2-characters of G, mapping S upon 1, then there exists to every element in $K/H(2)$, not in S, a C2-character in $P(S)$ which does not map it upon 1.*

If P_2 is the group of all the $C2$-characters of G, then we infer from (1) that $P_2/P(S)$ is essentially the same as the group of all the $C2$-characters of S. It follows from Theorem II.5.2 that the orders of S and of its group $P_2/P(S)$ of $C2$-characters are equal. If S'' is the group of elements in $K/H(2)$ mapped upon 1 by all the $C2$-characters in $P(S)$, then $S\leqq S''$ and $P(S)=P(S'')$ showing that S and S'' are of equal order; and this implies the desired equality of S and S''.

Assume now that every complete group of C-characters of G is 2-complete. Consider an element x of order 2 in $K/H(2)$; and denote by B_2 the group of all the $C2$-characters of G which map x upon 1, by Q the group of all the C-characters of odd order of G, and by B the product of Q and B_2. The group of elements in G, mapped upon 1 by Q, is $\overline{H}(2)$; and the group of elements in G mapped upon 1 by B_2 is, by (2), the group X, generated by the elements in the coset x of $K/H(2)$. Since B is obviously not 2-complete, it follows that B

([36]) Thus $H(2)\ \overline{H}(2)$ contains every element in G_{C2} whose order modulo $H(2)$ is 2; and it may happen that these are the only elements in K whose orders modulo $H(2)$ are 2.

is not complete; and this implies that the cross-cut of X and $\overline{H}(2)$ is different from 1. Since $X/H(2)$ is of order 2, and since the cross-cut of $H(2)$ and $\overline{H}(2)$ is 1 as a consequence of the C-completeness of G, it follows now that $X \leqq H(2)\overline{H}(2)$, proving the necessity of condition (i).

Suppose now that the order of G/G_{C2} is 4. If x is an element of order 2 in $G/H(2)$ which does not induce the inversion in $E(2)$, then it is a consequence of condition (i), already proven, that x is in $(\overline{H}(2)H(2))/H(2)$, provided x is in $K/H(2)$. If x is not in $K/H(2)$, then the integer corresponding to x under $C2$ is of the form $x \equiv -1+2^{m(2)-1}$ modulo $2^{m(2)}$. We denote by B_2 the group of all the $C2$-characters of G which map x upon 1; and by W the group, generated by adjoining x to $G_{C2}/H(2)$. From $x^2=1$ and Lemma I.3.4 we infer that every C_0-character of $G_{C2}/H(2)$ is induced by a $C2$-character of W which maps x upon 1; and it follows from Corollary III.1.3 and the fact that W is of index 2 in $G/H(2)$ that every $C2$-character of W is induced by a $C2$-character of $G/H(2)$. Since B_2 contains the $C2$-character which maps W upon 1 and the elements in $G/H(2)$ which are not in W upon the element of order 2 in $E(2)$, it follows that only elements in W are mapped upon 1 by B_2. Since every C_0-character of $G_{C2}/H(2)$ is induced by a $C2$-character in B_2, and since $G/H(2)$ is $C2$-complete, it follows that elements not equal to 1 in $G_{C2}/H(2)$ are not mapped upon 1 by every $C2$-character in B_2. Thus it follows that x and 1 are the only elements mapped upon 1 by every $C2$-character in B_2. Denote now by Q the group of all the C-characters of odd order of G, and by B the product of Q and B_2. If we denote by X the subgroup consisting of the elements in $H(2)$ and in the coset x, then the cross-cut of X and $\overline{H}(2)$ is the set of elements mapped upon 1 by B. Since B is not 2-complete, it follows that B is not complete and that therefore the cross-cut of X and $\overline{H}(2)$ is not 1. Since $X/H(2)$ is of order 2, this implies $X \leqq H(2)\overline{H}(2)$, that is, we have verified the necessity of condition (ii').

Suppose again that G/G_{C2} is of order 4. Then G may be generated by adjoining to K the elements in G which induce the inversion in $E(2)$. Assume furthermore that the element z in $G/H(2)$ induces the inversion in $E(2)$ and satisfies $(zy)^2=y^{2^{m(2)-1}}$ for every y in $K/H(2)$ which is not in $G_{C2}/H(2)$. Then it follows from Lemma IV.3.1(c) that every $C2$-character f of $G/H(2)$ satisfies

$$\begin{aligned} f(z)^{1-y} &= f([z, y])^y f(y)^2 = f(zyzyy^{-2})^y f(y)^2 = f(y^{2^{m(2)-1}-2})^y f(y)^2 \\ &= f(y^2)^{y(2^{m(2)-2}-1)} f(y)^2 = f(y)^{(1+y)y(2^{m(2)-2}-1)} f(y)^2 \\ &= f(y)^{(y+1)(2^{m(2)-2}-1)} f(y)^2 \\ &= f(y)^{2(1+2^{m(2)-2})(2^{m(2)-2}-1)} f(y)^2 = f(y)^{-2} f(y)^2 = 1; \end{aligned}$$

and it follows from Corollary III.1.3 that every $C2$-character of $K/H(2)$ is induced by a $C2$-character of $G/H(2)$ which maps z upon 1. If we denote by B_2 the group of all the $C2$-characters of G which map the coset z of $G/H(2)$

upon 1, then it is readily seen that the subgroup X, generated by the elements in the coset z and containing $H(2)$, consists exactly of the elements in G mapped upon 1 by the $C2$-characters in B_2, since $K/H(2)$ is $C2$-complete. Denote by Q again the group of C-characters of odd order of G. Then $\overline{H}(2)$ is the set of elements mapped upon 1 by Q. The group $B=QB_2$ is not 2-complete; and thus it follows that B is not complete. This implies that the cross-cut of $\overline{H}(2)$ and X is different from 1; and we deduce $X \leqq H(2)\overline{H}(2)$ from the fact that $X/H(2)$ is of order 2, proving the necessity of condition (ii'').

We assume now conversely that the conditions (i) and (ii) are satisfied by G, C, and that B is a complete group of C-characters of G. This group B is the direct product of the groups B_2 and P where P consists of the C-characters of odd order in B whereas B_2 is the subgroup of all the $C2$-characters in B. We denote by R a group between K and G whose elements do not induce the inversion in $E(2)$ and whose index in G is 2. If x is an element of order 2 in $R/H(2)$, then x is in $K/H(2)$, since $R/H(2)$ is cyclic. Consequently we may deduce from condition (i) that x is in $(\overline{H}(2)H(2))/H(2)$. There exists therefore an element $w \neq 1$ in $\overline{H}(2)$ such that $x=H(2)w$. From the completeness of B we infer the existence of a $C2$-character b in B_2 which does not map w upon 1. Hence $b(x)=b(w)\neq 1$, showing that B_2 induces a complete group of $C2$-characters in $R/H(2)$. Thus we may deduce from Theorem IV.2.2 that every $C2$-character of $R/H(2)$ is induced by some $C2$-character in B_2.

If s is an element of order 2 in $G/H(2)$, and if s is in $R/H(2)$, then we have already shown that $B_2(s)\neq 1$. If s is not in $R/H(2)$, then we distinguish two cases.

Case 1. *s does not induce an inversion in $E(2)$.* Then there exists an element g generating $R/H(2)$ modulo $G_{C2}/H(2)$ and an inversion z in $G/H(2)$ such that $s=zg^{2^i}$ for some i. Since s is not an inversion, g^{2^i} is not in $G_{C2}/H(2)$. Since s is of order 2, we find that

$$1 = s^2 = (zg^{2^i})^2 = zg^{2^i}zg^{-2^i}g^{2^i} = [z, g^{2^i}]g^{2^{i+1}},$$

$$g^{2^{i+1}} = [g^{2^i}, z],$$

since inversions are induced in $E(2)$ by elements of order 2 in $G/H(2)$, as follows from Theorem III.1.2. Thus it follows that the automorphism g^{2^i} of $E(2)$ is of order 2, that g^{2^i} is therefore in $K/H(2)$, and that the integer corresponding under $C2$ to the element g^{2^i} in $K/H(2)$ is $g^{2^i}\equiv 1+2^{m(2)-1}$ modulo $2^{m(2)}$.

Every $C2$-character of $R/H(2)$ is induced by some $C2$-character in B_2. Thus there exists a $C2$-character f in B_2 such that $f(t)=e^{1-t}$ for t in $R/H(2)$ where e is an element generating $E(2)$. If $0<i$, then the order of $g^{2^{i+1}}$ does not exceed $2^{m(2)-i-1}$ which is a divisor of $2^{m(2)-2}$; and thus it follows from Corollary III.1.3 that $f(z)$ is of the form $e^{2+f_0 2^{m(2)-2}}$, generates $E(2)^2$. Consequently we find that $f(zg^{2^i})=f(z)^{g^{2^i}}f(g^{2^i})=f(z)^{1+2^{m(2)-1}}e^{2^{m(2)-1}}\neq 1$, since the second factor

is of order 2, the first is of order $2^{m(2)-1}$, that is $B_2(s)\neq 1$. If, however, $i=0$, then g^2 is in $G_{C2}/H(2)$ and the order of G/G_{C2} is 4. In this case we infer from condition (ii') that s is in $(\overline{H}(2)H(2))/H(2)$; and there exists an element s'' in $\overline{H}(2)$ such that $s=H(2)s''$. Since B is complete, and since $P(\overline{H}(2))=1$, there exists a $C2$-character d in B_2 such that $d(s)=d(s'')\neq 1$; and we have shown again that $B_2(s)\neq 1$.

Case 2. An inversion is induced by s in $E(2)$. Then we consider again an element g in $R/H(2)$ which generates R modulo G_{C2}. There exists a $C2$-character f in B_2 such that $f(t)=e^{1-t}$ for t in $R/H(2)$ where the element e generates $E(2)$. It follows from Lemma IV.3.1(c) that $f(s)^{1-g}=e^{2(g-1)}$; and this implies $f(s)\neq 1$, provided the automorphism g of $E(2)$ is not of order 2; $B_2(s)\neq 1$ provided G/G_{C2} is not of order 4.

If G/G_{C2} is of order 4, then it may happen that there exists a $C2$-character f of $R/H(2)$ such that $f([s, g])^g f(g)^2\neq 1$. This $C2$-character is induced by some $C2$-character f in B_2; and it follows from Lemma IV.3.1(c) that $f(s)^{1-g}\neq 1$ so that again $B_2(s)\neq 1$.

Suppose finally that $1=f([s, g])^g f(g)^2$ for every $C2$-character f of $R/H(2)$. Then we note that the integer corresponding to g under $C2$ is $g\equiv 1+2^{m(2)-1}$ modulo $2^{m(2)}$, since g induces an automorphism of order 2 in $E(2)$, and since g is in $R=K$. Consequently we find:

$$\begin{aligned} f((sg)^2 g^{-2^{m(2)-1}}) &= f(sgsg^{-1}g^{2-2^{m(2)-1}}) = f([s, g])f(g^{2-2^{m(2)-1}}) \\ &= f([s, g])f(g^2)^{1-2^{m(2)-2}} \qquad \text{(since } g^2 \text{ is in } G_{C2}/H(2)\text{)} \\ &= f([s, g])f(g)^{(1+g)(1-2^{m(2)-2})} \\ &= f([s, g])f(g)^2 = f([s, g])^g f(g)^2 = 1, \end{aligned}$$

since $f([s, g])$ is of an order dividing $2^{m(2)-1}$, and we infer from the $C2$-completeness of $G/H(2)$ that $R/H(2)$ is $C2$-complete, and that therefore $(sg)^2=g^{2^{m(2)-1}}$. Since g may be any element in $R/H(2)=K/H(2)$ which is not in $G_{C2}/H(2)$, we may apply condition (ii); and it follows that s is in $(\overline{H}(2)H(2))/H(2)$; and there exists an element s_0 in $\overline{H}(2)$ such that $s=H(2)s_0$. Since B is complete, we have $B(s_0)\neq 1$. Since s_0 is in $\overline{H}(2)$, we have $Q(s_0)=1$. Hence there exists a $C2$-character b in B_2 such that $b(s)=b(s_0)\neq 1$, proving again that $B_2(s)\neq 1$.

Thus we have finally shown that $B_2(s)\neq 1$ for every s in G whose order modulo $H(2)$ is exactly 2; and that proves the 2-completeness of B, as was to be shown.

For the enunciation of the next theorem we need a restatement of a concept introduced before (cp. Lemma IV.3.4!): If G/G_{C2} is not cyclic, then there exists one and only one subgroup $A=A(G, C)$ which contains G_{C2}, is of index 2 in G, does not contain any element inducing the inversion in $E(2)$, and contains an element such that the integer corresponding to it under C_2 is congruent to -1 modulo 4.

THEOREM IV.4.5. *If G is C-complete, then the following conditions are necessary and sufficient for the full C-character group of G to be the only complete group of C-characters of G:*

(a) *If G/G_{Cp} is cyclic, then $\overline{H}(p)H(p)$ contains every element in G whose order* modulo $H(p)$ *is p.*

(b) *If G/G_{Cp} is of order prime to p, and if the element x in G is* modulo $H(p)$ *of order a prime number different from p, then $\overline{H}(p)H(p)$ contains an element y which is not in $H(p)$, but satisfies $xy \equiv yx$* modulo $H(p)$.

(c) *If G/G_{C2} is not cyclic, then $\overline{H}(2)H(2)$ contains every element in the subgroup K (introduced in Theorem* IV.4.4) *whose order* modulo $H(2)$ *is* 2.

(d) *If p is odd and $G \neq G_{Cp}$, then either $m(p)=1$ or the order of G/G_{Cp} is divisible by p.*

(e) *If G/G_{C2} is of order* 2, *and if there exists an element in G to which there corresponds under $C2$ an integer congruent to* -1 modulo 4, *then $H(2)G_{C2}^2 < H(2)G^2$.*

(f) *If G/G_{C2} is not cyclic, and if the order of G/G_{C2} is divisible by* 8, *then $H(2)$ G' is not part of $A^2H(2)$.*

(g) *If G/G_{C2} is not cyclic, but of order* 4, *then neither $H(2)G'$ nor $H(2)A^2$ is equal to $H(2)G_C^2$.*

Proof. It is readily seen that the following two conditions are necessary and sufficient for the full C-character group of G to be the only complete group of C-characters of G:

(A) Every complete group of C-characters of G is p-complete, for every prime p.

(B) The full Cp-character group of G (or of $G/H(p)$) is the only complete group of Cp-characters of $G/H(p)$, for every prime p.

It is an immediate consequence of Theorems IV.2.2 and IV.3.7 that the conditions (d) to (g) of the theorem are equivalent to the property (B); and it is a consequence of Theorems IV.4.3 and IV.4.4 that (A) implies conditions (a) to (c). If conversely all the conditions (a) to (g) are satisfied by G and C, then the conditions (p*) and (p**) of Theorem IV.4.3 are consequences of (a) and (b) respectively; and condition (i) of Theorem IV.4.4 is an immediate consequence of the present condition (c). Condition (ii'') of Theorem IV.4.4 is satisfied, since we may infer from (g) the impossibility of the existence of an element z meeting the requirements of condition (ii'') of Theorem IV.4.4 considering that $2 < m(2)$, if G/G_{C2} is not cyclic. Condition (ii') of Theorem IV.4.4 is a consequence of condition (c) of the present theorem, since elements of order 2 in $G/H(2)$ which do not induce the inversion in $E(2)$ belong by Theorem IV.4.5(i) and Lemma IV.3.4 to $K/H(2)$, if the order of G/G_{C2} is 4 and G/G_{C2} is not cyclic. Thus it follows from Theorems IV.4.3 and IV.4.4 that condition (A) is a consequence of the conditions (a) to (g); and this completes the proof.

CHAPTER V. DUALITY

A *projectivity* of the group S upon the group T is a biunivoque correspondence which maps the set of all the subgroups of S upon the set of all the subgroups of T and which has the property of preserving the relation "$\leqq$." A *duality* of the group S upon the group T is a biunivoque correspondence which maps the set of all the subgroups of S upon the set of all the subgroups of T and which has the property of inverting the relation "$\leqq$." If the product of two dualities exists, then it is a projectivity.

If G is a group and C a homomorphism of G into the group of automorphisms of the cyclic group E of order m, then we denote the *C-character group of* G by $L=L(G, C)$. This group L is an abelian group the orders of whose elements are divisors of m; and thus it follows from Theorems I.1.3 and I.1.4 that L and the group L_0 of its C_0-characters in E are isomorphic groups; and that there exists a duality between L and L_0. Thus the problems of constructing a duality between G and L and that of constructing a projectivity between G and L_0 are equivalent problems.

V.1. **The natural projectivity between G and L_0.** Throughout this section we make use of the notations (II.3.*). In the proof of Theorem IV.1.2 we have introduced the operator F_g, defined by the equation $F_g(f)=f(g)$ for g an element in G and f a C-character of G.

LEMMA V.1.1. *Suppose that G is C-complete.*

(a) *F_g is a C_0-character of the C-character group of G, that is F_g is, for every g in G, an element in L_0.*

(b) *If s and t are elements in G such that $F_s=F_t$, then $s=t$.*

(c) *If S is a subset of G such that the set F_S is a subgroup of L_0, then S is a subgroup of G.*

REMARK. Note that F_G need not be a subgroup of L_0, though F_G is always a subset of L_0. In this respect see Theorem V.1.2.

Proof. Statements (a) and (b) are easily verified; see for example (I.3.5.1) and (I.3.5.2). Suppose now that S is a subset of G such that F_S is a subgroup of L_0, and that s, t are elements in S. Then the characters F_s, F_t, F_s^t and $F_s^tF_t$ belong to F_S. If f is any C-character of G, then $F_s^tF_t(f)=(F_s(f))^tF_t(f)=f(s)^tf(t)=f(st)=F_{st}(f)$; and it follows from (b) that st is in S, proving (c).

THEOREM V.1.2. *If G is C-complete, then each of the following properties implies the others:*

(1) *The set F_G is a group of C_0-characters of $L(G, C)$.*

(2) *C is regular.*

(3) *F_S is a group of C_0-characters of $L(G, C)$ if, and only if, S is a subgroup of G.*

REMARK. It is readily deduced from Lemma V.1.1 that F_S is a projectivity of G upon L_0 if, and only if, (3) holds true.

Proof. It is obvious that (1) is a consequence of (3). If (1) is satisfied by G, then F_G is a complete group of C_0-characters of $L(G, C)$, since $F_g(f)=1$ for every g implies $f(g)=1$ for every g, that is, implies $f=1$. Hence it follows from Theorem I.1.4 that F_G is the group L_0 of all the C_0-characters of $L(G, C)$ in E. It follows from Theorem I.1.3 and Lemma V.1.1(b) that G, $F_G=L_0$, and L are of equal order, and it follows from Corollary II.5.3(b) that (2) is a consequence of (1). Suppose finally that (2) is satisfied by G and C. Then we deduce from Lemma V.1.1(c) that we need prove only the following fact: F_S is a group, whenever S is a group. If S is a subgroup of G, then S is C-complete and satisfies the same condition (2) as G. Hence it follows from Corollary II.5.3(b) that S and its C-character group $L(S, C)$ are of equal order. Since $L(G, C)$ induces in S a complete group of C-characters, and since it follows from Theorem IV.1.2 that the C-character group of S is the only complete group of C-characters of S, we find that every C-character of S is induced by some C-character of G. If we denote by L_S the group of all the C-characters of G which map S upon 1, then it follows that $L(S, C)$ is essentially the same as $L(G, C)/L_S$; and since $L(S, C)$ and S, $L(G, C)$ and G are of equal order, we deduce that the order of L_S is the index $[G:S]$ of S in G. Denote by L_S^* the group of all the C_0-characters of $L(G, C)$ in E which map L_S upon 1. It is obvious that $F_S \leqq L_S^*$, since $f(S)=1$ and $F_S(f)=1$ are equivalent statements. It is a consequence of Theorems I.1.3 and I.1.4 that the order of L_S^* is the index of the subgroup L_S of $L(G, C)$ in $L(G, C)$. Since G and $L(G, C)$ are of equal order, and since the order of L_S is $[G:S]$, it follows that S and L_S are of equal order, proving that $F_S=L_S^*$, since F_S contains by Lemma V.1.1(b) as many elements as S. Since L_S^* is a group of C_0-characters of $L(G, C)$, it follows now that F_S is a group of C_0-characters of $L(G, C)$, as was to be shown.

THEOREM V. 1. 3. *The C-complete group G and its C-character group L are isomorphic if, and only if, G is abelian and C is regular.*

Proof. If G and L are isomorphic, then G is commutative, since L is commutative. Both groups furthermore have equal order and the regularity of C is a consequence of Corollary II.5.3.

Suppose conversely that G is commutative and that C is regular. Then it follows from Theorem V.1.2 that a projectivity of G upon L_0 is effected by mapping the subgroup S of G upon the subset F_S of L_0. Since S and F_S are groups of equal order, it may be deduced from a well known theorem([37]) that

([37]) See Rottländer, Math. Zeit. vol. 28 (1928) pp. 641–653 or R. Baer, Amer. J. Math. vol. 61 (1938) p. 30; one may verify this fact readily by showing the equality of the invariants of G and L_0.

G and L_0 are isomorphic. We infer from Theorem I.1.3 that L and L_0 are isomorphic, proving that G and L are isomorphic too.

V.2. **The natural duality between G and L.** The following procedure is customary for setting up a duality between groups and their character groups: using the notations (II.3.*) and assuming that G be C-complete, we denote by (L, S), for S a subgroup of G, the set of all the C-characters of G which map S upon 1; and we denote by (G, T), for T a subgroup of the C-character group L of G, the set of all the elements x in G, satisfying $T(x)=1$. Clearly (L, S) is a subgroup of L and (G, T) a subgroup of G; and it is readily verified that these correspondences effect dualities if, and only if,

(V.2.1) $(L, (G, T))=T$ *and* $(G, (L, S))=S$ *for every subgroup* S *and* T *of* G *and* L *respectively.*

It is our object to determine those G, C which meet the requirement (V.2.1). It is easy to see for example that the groups G, satisfying condition (3) of Theorem V.1.2, have the property (V.2.1).

THEOREM V.2.2. *If G is C-complete, then the following conditions are necessary and sufficient for G, C to satisfy* (V.2.1):

(i) *The orders of $H(p)$ and of $G/H(p)$ are relatively prime.*

(ii) *If the order of G/G_{Cp} is not a power of p, then $m(p)=1$ and the order of G/G_{Cp} is a prime (dividing $p-1$).*

(iii) *$C2$ is regular.*

Proof. Suppose first that (V.2.1) is satisfied by G and C. Denote by L_p the group of Cp-characters of G. Then $H(p)=(G, L_p)$ is nothing but a restatement of the definition of $H(p)$. We deduce from (V.2.1) that $L_p=(L, H(p))$ and that therefore the full Cp-character group L_p of $G/H(p)$ is the only complete group of Cp-characters of $G/H(p)$. Hence we infer from Theorem IV.2.2(1) that either the order of G/G_{Cp} is divisible by p or $G=G_{Cp}$ or $m(p)=1$. Denote by P_p the Cp-principal genus of G (or $G/H(p)$). Then $G_{Cp}=(G, P_p)$ and we deduce from (V.2.1) that $P_p=(L, G_{Cp})$. Applying this last result on $p=2$, we infer from Theorem II.3.2 that $C2$ cannot be singular. Every G/G_{Cp} is therefore cyclic. Since P_p is by Theorem II.2.1 a cyclic group of order a power of p, we may infer from (V.2.1) that G/G_{Cp} is a cyclic group of prime power order, containing as many subgroups as does P_p; and the necessity of the conditions (ii) and (iii) is now an immediate consequence of Theorem II.2.1.

Since L is the direct product of all the L_p, we find that $\overline{H}(p)=(G, \prod_{p\neq q}L_q)$; since the cross-cut of L_p and $\prod_{p\neq q}L_q$ is 1, then G is the product of $H(p)$ and $\overline{H}(p)$ (for every p); and this proves that G is the direct product of all the $\overline{H}(p)$. Since the orders of L_p and $\prod_{p\neq q}L_q$ are relatively prime, it follows that every subgroup T of L is the cross-cut of TL_p and of $T\prod_{p\neq q}L_q$; and hence it follows from (V.2.1) that every subgroup S of G is the product of its cross-cut with $H(p)$ and of its cross-cut with $\overline{H}(p)$, proving that the orders of

$H(p)$ and $\overline{H}(p)$ are relatively prime; and thus we have verified the necessity of (i).

Suppose conversely that the conditions (i) to (iii) are satisfied by G and C. Then we infer from (i) and Corollary II.4.4 that G is the direct product of its subgroups $\overline{H}(p)$; and that G is, for every prime p, the direct product of $H(p)$ and $\overline{H}(p)$.

Consider a subgroup S of $\overline{H}(p)$. Since every C-character of G maps $\overline{H}(p)$ into $E(p)$, it follows that $\overline{H}(p)$ and S are mapped upon 1 by every Cq-character for $q \neq p$; and since G is the direct product of $H(p)$ and $\overline{H}(p)$, it is readily seen that the C-characters of G induce in $\overline{H}(p)$ a group of Cp-characters which is essentially the same as the group L_p of the Cp-characters of G. Thus $(L, S) = (L, S)_p L_p'$ where $L_p' = \prod_{p \neq q} L_q$ and where $(L, S)_p$ is the group of Cp-characters of G which map S upon 1; and this shows that $(G, (L, S))$ is exactly the cross-cut of $(G, (L, S)_p)$ and $\overline{H}(p)$, that is $(G, (L, S))$ consists of those elements in $\overline{H}(p)$ which are mapped upon 1 by the Cp-characters in (L, S). If the order of G/G_{Cp} is a power of p, then we infer from (iii) the regularity of Cp and it follows from Theorem V.1.2 that $S = (G, (L, S))$. If the order of G/G_{Cp} is not a power of p, then it follows from (ii) that $m(p) = 1$ and that G/G_{Cp} is of order a prime $p^* \neq p$. Consequently either $S \leqq \overline{H}(p)_{Cp}$ or $\overline{H}(p) = S\overline{H}(p)_{Cp}$; in the first of these cases our contention $S = (G, (L, S))$ is an immediate consequence of Theorems I.1.4 and I.3.1; in the second of these cases we infer from Lemma I.3.4 that every C_0-character of $\overline{H}(p)_{Cp}$ in $E(p)$ which maps S_{Cp} upon 1 is induced by a Cp-character in $(L, S)_p$; and $S = (G, (L, S))$ is a consequence of Theorem I.1.4

If S is a subgroup of G, and if S_p is the cross-cut of S and $\overline{H}(p)$ then S is the direct product of the S_p, since the orders of $H(p)$ and $\overline{H}(p)$ are relatively prime by (i). If f is a C-character of G, then f is the product of uniquely determined Cp-characters f_p. Since $f_p(H(p)) = 1$, it follows that $f(S) = 1$ if, and only if, $f_p(S_p) = 1$ for every p. This shows that (L, S) is the direct product of the groups $(L, S_p)_p$ consisting of all the Cp-characters of G which map S_p upon 1. But we have shown in the preceding paragraph of the proof that $S_p = (G, L_p'(L, S_p)_p)$ and this makes the desired identity, $S = (G, (L, S))$ evident.

If T is a subgroup of the group L_p of the Cp-characters of G, then (G, T) contains $H(p)$, since $L_p(H(p)) = 1$. If f is a Cq-character of G for $q \neq p$ which maps $H(p)$ upon 1, then f maps $\overline{H}(p)$ upon 1 too; and this implies $f = 1$, since G is the direct product of $H(p)$ and $\overline{H}(p)$. Thus it follows that $(L, (G, T))$ is a group of Cp-characters of G. If the order of G/G_{Cp} is a power of p, then it follows from (iii) and Theorem V.1.2 that $T = (L, (G, T))$. If the order of G/G_{Cp} is not a power of p, then it follows from (ii) that $m(p) = 1$ and that G/G_{Cp} is of order a prime $p^* \neq p$. If the principal genus P_p of $G/H(p)$ in $E(p)$ is part of T, then (G, T) is between $H(p)$ and G_{Cp}; and it is readily verified that $T = (L, (G, T))$ by Theorems I.1.4 and I.3.1 and the fact that $(L, (G, T))$

is a group of Cp-characters. Thus we assume finally that P_p is not part of T. We note that P_p is of order p, and that every Cp-character of G different from 1 is of order p, since $E(p)$ is of order p. We wish to show that (G, T) contains an element not in G_{Cp}. Denote by g an element in $G/H(p)$, not in $G_{Cp}/H(p)$. Then g generates G modulo G_{Cp}, since G/G_{Cp} is of order a prime p^*; and it is a consequence of the Cp-completeness of $G/H(p)$ and of II.1.A and Theorem I.3.1 that p^* is the order of g. Our object is attained if g is in (G, T); and thus we assume that g is not in (G, T). We denote by T^* the subgroup of those Cp-characters in T which map g upon 1; since $E(p)$ is of order p, and since the Cp-characters of $G/H(p)$ therefore map g upon p different values, it follows that T/T^* is of order p. Since P_p is of order p, and since P_p is not part of T, it follows that the cross-cut of T and P_p is 1; and hence it follows from Theorem II.2.1(a) that different Cp-characters in T induce different C_0-characters of $G_{Cp}/H(p)$ in $E(p)$. Hence there exists an element in $G_{Cp}/H(p)$ which is mapped upon 1 by T^*, but not by T. Since the elements in $G_{Cp}/H(p)$ are of order p, this implies the existence of an element y in $G_{Cp}/H(p)$ such that the Cp-characters in T have the same values on g and on y. Consequently gy^{-1} is mapped upon 1 by the Cp-characters in T so that the elements in the coset gy^{-1} are in (G, T), though not in G_{Cp}. Denote now by w any element in (G, T), not in G_{Cp}. If f is a C-character in $(L, (G, T))$, then f is a Cp-character of G; and there follows from Theorem I.1.4 the existence of a Cp-character f^* in T which coincides with f on G_{Cp}. But both f and f^* map w upon 1; and G is generated by adjoining w to G_{Cp}. Hence $f=f^*$ is in T, proving the desired equation $T=(L, (G, T))$.

Consider now any subgroup T of L; and denote by T_p the group of the Cp-characters in T. Then T is the direct product of the subgroups T_p; and (G, T) is the cross-cut of the groups (G, T_p). Since (G, T_p) contains, as has been remarked before, the subgroup $H(p)$, it follows that (G, T_p) is the direct product of $H(p)$ and of a subgroup U_p of $\overline{H}(p)$, as G is the direct product of $H(p)$ and $\overline{H}(p)$. Since U_p is part of every $H(q)$ for $q\neq p$, it follows that U_p is part of (G, T). If f is a Cp-character in $(L, (G, T))$, than f maps both $H(p)$ and U_p upon 1 so that f belongs to $(L, (G, T_p))$. But we have shown in the preceding paragraph of the proof that $T_p=(L, (G, T_p))$ showing that f is in T; and now it is obvious that $T=(L, (G, T))$, as was to be shown.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.